

DOCKET NO.: 270750US90PCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Mitsuru KODAMA , et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP03/13126

INTERNATIONAL FILING DATE: October 14, 2003

FOR: COMMUNICATION SYSTEM AND TRANSFER DEVICE

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119  
AND THE INTERNATIONAL CONVENTION**Commissioner for Patents  
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

<b><u>COUNTRY</u></b>	<b><u>APPLICATION NO</u></b>	<b><u>DAY/MONTH/YEAR</u></b>
Japan	2002-303494	17 October 2002

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP03/13126. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Masayasu Mori  
Attorney of Record  
Registration No. 47,301  
Surinder Sachar  
Registration No. 34,423

Customer Number

**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

Rec'd PCT/PTO 18 APR 2003  
PCT/JP 03/13126

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

14.10.03

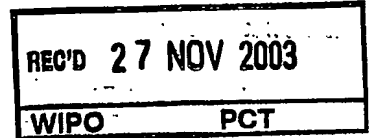
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2002年10月17日

出 願 番 号  
Application Number: 特願2002-303494  
[ST. 10/C]: [JP2002-303494]

出 願 人  
Applicant(s): 株式会社エヌ・ティ・ティ・ドコモ

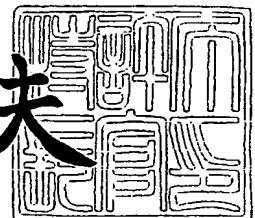


PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2003年11月14日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 DCMH140419

【提出日】 平成14年10月17日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 1/00

【発明の名称】 通信システム、転送装置、通信方法及びプログラム

【請求項の数】 10

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 児玉 充

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 辻 健次郎

【発明者】

【住所又は居所】 東京都千代田区永田町二丁目 1 1 番 1 号 株式会社エヌ  
・ ティ ・ ティ ・ ドコモ内

【氏名】 西村 一成

【特許出願人】

【識別番号】 392026693

【氏名又は名称】 株式会社エヌ ・ ティ ・ ティ ・ ドコモ

【代理人】

【識別番号】 100083806

【弁理士】

【氏名又は名称】 三好 秀和

【電話番号】 03-3504-3075

## 【選任した代理人】

【識別番号】 100100712

【弁理士】

【氏名又は名称】 岩▲崎▼ 幸邦

## 【選任した代理人】

【識別番号】 100095500

【弁理士】

【氏名又は名称】 伊藤 正和

## 【選任した代理人】

【識別番号】 100101247

【弁理士】

【氏名又は名称】 高橋 俊一

## 【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9702416

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信システム、転送装置、通信方法及びプログラム

【特許請求の範囲】

【請求項 1】 情報データを提供する情報提供手段と、

該情報提供手段が接続するアクセス制限がされた情報提供側ネットワークと、  
前記情報提供手段に対して前記情報データの提供を要求する要求データを送信して前記情報データを取得し、該取得した情報データを端末に送信する情報送信手段と、

該情報送信手段が接続するアクセス制限がされた情報送信側ネットワークと、  
該情報送信側ネットワークと前記情報提供側ネットワークとを接続し、前記情報送信側ネットワークを介して受信したデータが前記情報送信手段から送信されたデータであるか否か及び前記情報提供側ネットワークを介して受信したデータが前記情報提供手段から送信されたデータであるか否かを判断し、該判断結果に基づいて、前記情報送信側ネットワークを介して受信したデータ及び前記情報提供側ネットワークを介して受信したデータの転送を行う転送手段と  
を備えることを特徴とする通信システム。

【請求項 2】 前記情報提供側ネットワークは複数あり、該複数の情報提供側ネットワークにそれぞれ前記情報提供手段が接続し、

前記転送手段は、前記情報送信側ネットワークと前記複数の情報提供側ネットワークとを接続することを特徴とする請求項 1 に記載の通信システム。

【請求項 3】 前記転送手段は、前記情報送信手段から前記情報提供手段に送信されたデータに付加されているアドレスを、前記情報提供側ネットワークに適したアドレスに変換し、前記情報提供手段から前記情報送信手段に送信されたデータに付加されているアドレスを、前記情報送信側ネットワークに適したアドレスに変換することを特徴とする請求項 1 又は 2 に記載の通信システム。

【請求項 4】 前記転送手段は、前記情報送信手段から前記情報提供手段に送信されたデータに付加されているアドレスを、前記情報提供側ネットワークに適したアドレス及び前記情報送信側ネットワークに適したアドレス以外の共通アドレスに変換し、該変換した共通アドレスを前記情報提供側ネットワークに適し

たアドレスに変換し、前記情報提供手段から前記情報送信手段に送信されたデータに付加されているアドレスを前記共通アドレスに変換し、該変換した共通アドレスを前記情報送信側ネットワークに適したアドレスに変換することを特徴とする請求項 1 又は 2 に記載の通信システム。

【請求項 5】 前記転送手段は、前記情報提供手段からの情報データを同時に転送するデータ量の閾値を保持し、

前記情報提供側ネットワークを介して受信した前記情報提供手段から送信された情報データのデータ量と前記閾値とを比較し、該比較結果に基づいて前記データの転送を制御することを特徴とする請求項 1 乃至 4 のいずれか 1 項に記載の通信システム。

【請求項 6】 前記情報データは、映像データであることを特徴とする請求項 1 乃至 5 のいずれか 1 項に記載の通信システム。

【請求項 7】 前記情報提供側ネットワーク又は前記情報送信側ネットワークは、仮想閉域網であることを特徴とする請求項 1 乃至 6 のいずれか 1 項に記載の通信システム。

【請求項 8】 情報データを提供する情報提供手段と、該情報提供手段が接続するアクセス制限がされた情報提供側ネットワークと、前記情報提供手段に対して前記情報データの提供を要求する要求データを送信して前記情報データを取得し、該取得した情報データを端末に送信する情報送信手段と、該情報送信手段が接続するアクセス制限がされた情報送信側ネットワークとを備える通信システムにおいて用いられる転送装置であって、

前記情報送信側ネットワークと前記情報提供側ネットワークとを接続し、前記情報送信側ネットワークを介して受信したデータが前記情報送信手段から送信されたデータであるか否か及び前記情報提供側ネットワークを介して受信したデータが前記情報提供手段から送信されたデータであるか否かを判断し、該判断結果に基づいて、前記情報送信側ネットワークを介して受信したデータ及び前記情報提供側ネットワークを介して受信したデータの転送を行うことを特徴とする転送装置。

【請求項 9】 情報データを提供する情報提供手段と、該情報提供手段が接

続するアクセス制限がされた情報提供側ネットワークと、前記情報提供手段から取得した前記情報データを端末に送信する情報送信手段と、該情報送信手段が接続するアクセス制限がされた情報送信側ネットワークと、該情報送信側ネットワークと前記情報提供側ネットワークとを接続する転送手段とを備える通信システムにおいて用いられる通信方法であって、

前記情報送信手段が、前記情報提供手段に対して前記情報データの提供を要求する要求データを送信するステップと、

前記転送手段が、前記情報送信側ネットワークを介して受信した前記要求データが前記情報送信手段から送信された要求データであるか否かを判断し、前記受信した要求データが前記情報送信手段から送信された要求データである場合に、該要求データを前記情報提供側ネットワークを介して前記情報提供手段に転送するステップと、

前記情報提供手段が、前記要求データに基づいて前記情報データを前記情報送信手段に送信するステップと、

前記転送手段が、前記情報提供側ネットワークを介して受信した前記情報データが前記情報提供手段から送信された情報データであるか否かを判断し、前記受信した情報データが前記情報提供手段から送信された情報データである場合に、該情報データを前記情報送信側ネットワークを介して前記情報送信手段に転送するステップと

有することを特徴とする通信方法。

【請求項 10】 情報データを提供する情報提供手段と、該情報提供手段が接続するアクセス制限がされた情報提供側ネットワークと、前記情報提供手段に対して前記情報データの提供を要求する要求データを送信して前記情報データを取得し、該取得した情報データを端末に送信する情報送信手段と、該情報送信手段が接続するアクセス制限がされた情報送信側ネットワークとを備える通信システムにおいて用いられるコンピュータに、

前記情報送信側ネットワークと前記情報提供側ネットワークとを接続し、前記情報送信側ネットワークを介して受信したデータが前記情報送信手段から送信されたデータであるか否か及び前記情報提供側ネットワークを介して受信したデー

タが前記情報提供手段から送信されたデータであるか否かを判断し、該判断結果に基づいて、前記情報送信側ネットワークを介して受信したデータ及び前記情報提供側ネットワークを介して受信したデータの転送を行う転送手段として機能させるためのプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信システム、転送装置、通信方法及びプログラムに関する。

【0002】

【従来の技術】

従来、映像データをストリーミング方式により携帯端末に送信する通信システムがある（例えば、非特許文献1参照）。又、そのようなストリーミング方式による映像データの送信を行う通信システムとして、例えば、図11に示すものが用いられている。図11に示す通信システム401では、映像を撮影するカメラ410と、携帯端末440に映像データをストリーミング方式により送信するストリーミングサーバ430とが、1つの仮想閉域網（Virtual Private Network、以下「VPN」という）420に接続し、そのVPN420を介して接続している。通信システム401では、カメラ410が、映像データをVPN420を介してストリーミングサーバ430に送信する。そして、ストリーミングサーバ430が、カメラ410から送信された映像データを取得し、携帯端末440に送信する。このような通信システム401によれば、カメラ410とストリーミングサーバ430とが1つのVPN420に接続しているため、カメラ410からストリーミングサーバ430までのセキュリティが確保されるというメリットがある。

【0003】

【非特許文献1】

立川敬二 監修，「W-CDMA移動通信方式」，丸善株式会社，平成13年6月25日，p. 357～360

【0004】



**【発明が解決しようとする課題】**

しかしながら、従来の通信システム401では、カメラ410とストリーミングサーバ430は、1つのVPN420に接続してデータをやりとりする。そのため、映像データを提供する側のカメラ410と、その映像データを取得して端末に送信する側のストリーミングサーバ430と、VPN420とが、セキュリティポリシーやアドレス体系を統一しておく必要があった。

**【0005】**

又、カメラ410とストリーミングサーバ430は、1つのVPN420に接続するため、映像データを提供する側のカメラ410から、その映像データを取得して端末に送信する側のストリーミングサーバ430までのセキュリティを確保したいグループ毎に、カメラ410とストリーミングサーバ430が接続するVPN420をそれぞれ設ける必要があった。その結果、そのようなVPN420を構築するために、コストが非常に高くなってしまう問題があった。特に、セキュリティを確保したいグループが多数存在する場合には、その数だけカメラ410とストリーミングサーバが接続するVPN420を構築する必要が生じ、コストが高くなる問題が顕著であった。

**【0006】**

そこで、本発明は、情報データを提供する情報提供側と、その情報提供側から取得した情報データを端末に送信する情報送信側とが、独自のセキュリティポリシーを保つことができ、低コストで構築可能なセキュリティの高い通信システム及びその通信システムを用いた通信方法、並びに、その通信システムで用いられる転送装置及びプログラムを提供することを目的とする。

**【0007】****【課題を解決するための手段】**

本発明に係る通信システムは、情報データを提供する情報提供手段と、その情報提供手段が接続するアクセス制限がされた情報提供側ネットワークと、情報提供手段に対して情報データの提供を要求する要求データを送信して情報データを取得し、その取得した情報データを端末に送信する情報送信手段と、その情報送信手段が接続するアクセス制限がされた情報送信側ネットワークと、情報送信側

ネットワークと情報提供側ネットワークとを接続し、情報送信側ネットワークを介して受信したデータが情報送信手段から送信されたデータであるか否か及び情報提供側ネットワークを介して受信したデータが情報提供手段から送信されたデータであるか否かを判断し、その判断結果に基づいて、情報送信側ネットワークを介して受信したデータ及び情報提供側ネットワークを介して受信したデータの転送を行う転送手段とを備えることを特徴とする。

#### 【0008】

このような本発明に係る通信システムによれば、情報提供手段はアクセス制限がされた情報提供側ネットワークに接続し、情報送信手段はアクセス制限がされた情報送信側ネットワークに接続して、情報提供手段と情報送信手段は、それぞれ異なるネットワークに接続する。そして、転送手段は、情報送信側ネットワークを介して受信したデータが情報送信手段から送信されたデータであるか否かを判断し、情報提供側ネットワークを介して受信したデータが情報提供手段から送信されたデータであるか否かを判断し、それらの判断結果に基づいて、情報送信側ネットワークを介して受信したデータや情報提供側ネットワークを介して受信したデータの転送を行う。

#### 【0009】

そのため、情報送信手段と情報提供手段が両方とも接続するような、セキュリティポリシーの統一された1つのネットワークを構築する必要がない。よって、情報送信手段及び情報送信側ネットワークと、情報提供手段及び情報提供側ネットワークは、それぞれ独自のセキュリティポリシーを保ったまま、転送手段を介して接続することができる。又、転送手段が、情報送信側ネットワークや情報提供側ネットワークを介して受信したデータが、それぞれ情報送信手段や情報提供手段から送信されたデータであるか否かを判断し、その判断結果に基づいてデータの転送を行う。よって、情報送信手段及び情報送信側ネットワークと、情報提供手段及び情報提供側ネットワークとの間では、情報送信手段又は情報提供手段から送信されたデータという特定のデータのみがやりとりされる。更に、情報提供側ネットワーク、情報送信側ネットワークはそれぞれアクセス制限がされている。これらの結果、通信システムは高いセキュリティを確保できる。

## 【 0 0 1 0 】

又、情報送信手段と情報提供手段が両方とも接続するような、セキュリティポリシーの統一された1つのネットワークを構築する必要がある結果、情報送信手段が接続する情報送信側ネットワークや情報提供手段が接続する情報提供側ネットワークとして既存のものがあれば、それらをそのまま利用して通信システムを構築できる。よって、低コストで効率的に通信システムを構築することができる。

## 【 0 0 1 1 】

又、情報提供側ネットワークは複数あり、その複数の情報提供側ネットワークにそれぞれ情報提供手段が接続し、転送手段は、情報送信側ネットワークと複数の情報提供側ネットワークとを接続するようにしてもよい。これによれば、転送手段を介して、情報送信側ネットワークと、複数の情報提供側ネットワークとを接続することができる。よって、情報提供手段から情報送信手段までのセキュリティを確保したいグループが多数存在する場合であっても、情報提供側ネットワークをセキュリティを確保したいグループの数だけ設ければ、セキュリティを確保したいグループの数の情報送信側ネットワークを設ける必要はない。又、情報送信手段と情報提供手段が両方とも接続するような1つのネットワークを、セキュリティを確保したいグループの数だけ設ける必要もない。よって、情報データを提供する情報提供側と情報送信側とが、独自のセキュリティポリシーを保つことができる通信システムを、より低コストで構築することができる。

## 【 0 0 1 2 】

更に、転送手段は、情報送信手段から情報提供手段に送信されたデータに付加されているアドレスを、情報提供側ネットワークに適したアドレスに変換し、情報提供手段から情報送信手段に送信されたデータに付加されているアドレスを、情報送信側ネットワークに適したアドレスに変換することが好ましい。又、転送手段は、情報送信手段から情報提供手段に送信されたデータに付加されているアドレスを、情報提供側ネットワークに適したアドレス及び情報送信側ネットワークに適したアドレス以外の共通アドレスに変換し、その変換した共通アドレスを情報提供側ネットワークに適したアドレスに変換し、情報提供手段から情報送信

手段へのデータに付加されているアドレスを共通アドレスに変換し、その変換した共通アドレスを情報送信側ネットワークに適したアドレスに変換するようにしてもよい。

#### 【0013】

これらによれば、情報送信手段及び情報送信側ネットワークと、情報提供手段及び情報提供側ネットワークは、それぞれ独自のアドレス体系を保ったまま、転送手段を介して接続することができる。その結果、通信システムは、アドレス体系の統一を行う必要がなく、より低コストで通信システムを構築することができる。

#### 【0014】

更に、転送手段は、情報提供手段からの情報データを同時に転送するデータ量の閾値を保持し、情報提供側ネットワークを介して受信した情報提供手段から送信された情報データのデータ量と閾値を比較し、その比較結果に基づいてデータの転送を制御することが好ましい。これによれば、情報送信側ネットワークや情報提供側ネットワーク、転送手段、情報送信手段の処理能力や情報送信手段が情報データを送信する際の品質、情報データを受信する端末の数等に応じて閾値を定めることにより、通信システムは、ネットワークや転送手段の処理能力、提供する情報データの品質、端末の数等に応じたデータの転送を行うことができる。

#### 【0015】

又、通信システムでは、情報データとして、映像データをやりとりすることが好ましい。本発明に係る通信システムでは、情報送信手段及び情報送信側ネットワークと、情報提供手段及び情報提供側ネットワークとの間では、情報送信手段又は情報提供手段から送信されたデータという特定のデータのみがやりとりされる。そのため、情報送信手段は、映像データのように容量の大きいデータであっても、効率よく受信することができる。又、情報提供側ネットワーク又は前記情報送信側ネットワークは、仮想閉域網、即ち、VPNであることが好ましい。

#### 【0016】

又、本発明に係る転送装置は、情報データを提供する情報提供手段と、情報提供手段が接続するアクセス制限がされた情報提供側ネットワークと、情報提供手

段に対して情報データの提供を要求する要求データを送信して情報データを取得し、取得した情報データを端末に送信する情報送信手段と、情報送信手段が接続するアクセス制限がされた情報送信側ネットワークとを備える通信システムにおいて用いられる転送装置であって、情報送信側ネットワークと情報提供側ネットワークとを接続し、情報送信側ネットワークを介して受信したデータが情報送信手段から送信されたデータであるか否か及び情報提供側ネットワークを介して受信したデータが情報提供手段から送信されたデータであるか否かを判断し、その判断結果に基づいて、情報送信側ネットワークを介して受信したデータ及び情報提供側ネットワークを介して受信したデータの転送を行うことを特徴とする。

#### 【0017】

又、このような転送装置は、情報データを提供する情報提供手段と、情報提供手段が接続するアクセス制限がされた情報提供側ネットワークと、情報提供手段に対して情報データの提供を要求する要求データを送信して情報データを取得し、取得した情報データを端末に送信する情報送信手段と、情報送信手段が接続するアクセス制限がされた情報送信側ネットワークとを備える通信システムにおいて用いられるコンピュータに、情報送信側ネットワークと情報提供側ネットワークとを接続し、情報送信側ネットワークを介して受信したデータが情報送信手段から送信されたデータであるか否か及び情報提供側ネットワークを介して受信したデータが情報提供手段から送信されたデータであるか否かを判断し、その判断結果に基づいて、情報送信側ネットワークを介して受信したデータ及び情報提供側ネットワークを介して受信したデータの転送を行う転送手段として機能させるためのプログラムを実行させることにより実現できる。

#### 【0018】

又、本発明に係る通信方法は、情報データを提供する情報提供手段と、その情報提供手段が接続するアクセス制限がされた情報提供側ネットワークと、情報提供手段から取得した情報データを端末に送信する情報送信手段と、その情報送信手段が接続するアクセス制限がされた情報送信側ネットワークと、情報送信側ネットワークと情報提供側ネットワークとを接続する転送手段とを備える通信システムにおいて用いられる通信方法であって、情報送信手段が、情報提供手段に対

して情報データの提供を要求する要求データを送信するステップと、転送手段が、情報送信側ネットワークを介して受信した要求データが情報送信手段から送信された要求データであるか否かを判断し、受信した要求データが情報送信手段から送信された要求データである場合に、その要求データを情報提供側ネットワークを介して情報提供手段に転送するステップと、情報提供手段が、要求データに基づいて情報データを情報送信手段に送信するステップと、転送手段が、情報提供側ネットワークを介して受信した情報データが情報提供手段から送信された情報データであるか否かを判断し、受信した情報データが情報提供手段から送信された情報データである場合に、その情報データを情報送信側ネットワークを介して情報送信手段に転送するステップと有することを特徴とする。

#### 【0019】

このような本発明に係る通信方法によれば、情報提供手段及び情報提供側ネットワークと、情報送信手段及び情報送信側ネットワークは、それぞれ独自のセキュリティポリシーを保ったまま、高いセキュリティを確保して情報データの提供を要求したり、情報データを提供したりすることができる。

#### 【0020】

##### 【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら説明する。

#### 【0021】

##### 〔第1の実施の形態〕

##### (通信システム)

図1に示すように、本実施形態の通信システム1は、複数の映像提供部10と、提供側VPN20と、提供側サーバ30と、ルータ40と、送信側VPN50と、ストリーミングサーバ60と、複数の携帯端末70とを備えている。

#### 【0022】

映像提供部10は、情報データを提供する情報提供手段である。映像提供部10は、情報データとして映像データを提供する。映像提供部10は、映像データ等の情報データを提供する情報提供者から、映像データの受信の許可を受けたユーザが使用する携帯端末70にのみ映像データを提供する。尚、携帯端末70の

ユーザは、映像データを受信するためには、情報提供者から映像データの受信の許可を受けて、ユーザID、携帯端末70に固有の発ID、パスワード等を取得しておく。

#### 【0023】

映像提供部10は、カメラ11と映像提供サーバ12とを備える。カメラ11及び映像提供サーバ12は、例えば、エレベータや個人の住宅、マンション等の集合住宅、幼稚園、託児所、学校、公共施設、店舗、工事現場、観光地等、リアルタイムの映像を視聴したい複数の場所に設置される。そのため、映像データには、例えば、エレベータや住宅、集合住宅、幼稚園、託児所、学校、公共施設、店舗、工事現場、観光地等のリアルタイムの映像データがある。このように、映像データには、警備目的のデータや企業内のデータ等がある。映像提供部10は、ストリーミングサーバ60からの映像データの提供の要求や指示に応じて、映像データをストリーミングサーバ60に提供する。映像提供部10は、提供側VPN20に接続する。そして、映像提供部10は、提供側VPN20、ルータ40、送信側VPN50を介して、ストリーミングサーバ60に映像データを送信する。

#### 【0024】

提供側VPN20は、情報提供手段である映像提供部10が接続するアクセス制限がされた情報提供側ネットワークである。提供側VPN20は、ルータ40に接続し、ルータ40を介して送信側VPN50と接続する。提供側VPN20は、認証サーバ21を備える。認証サーバ21は、提供側VPN20にアクセスしようとする映像提供部10、提供側サーバ30、その他の端末に対して、ユーザIDやパスワード、発ID等を用いた認証を行って、アクセスを制限する。そのため、映像提供部10や提供側サーバ30も、最初に提供側VPN20にアクセスして接続を確立する際には認証処理を受ける。尚、認証は、例えば、発IDのみを用いて行ってもよく、ユーザIDとパスワードを用いて行ってもよく、ユーザIDとパスワードと発IDを用いて行ってもよい。提供側サーバ30は、提供側VPN20に接続するサーバである。提供側サーバ30は、様々な情報処理を行う。

**【0025】**

情報提供部10と、提供側VPN20と、提供側サーバ30は、同じセキュリティポリシーを持ち、同じ体系のアドレスを用いる。情報提供者により、独自のセキュリティポリシー、独自のアドレス体系で統一された情報提供部10と、提供側VPN20と、提供側サーバ30とが構築される。

**【0026】**

ストリーミングサーバ60は、情報提供手段である映像提供部10に対して映像データの提供を要求する要求データを送信して情報データとして映像データを取得し、その取得した映像データを携帯端末70に送信する情報送信手段である。ストリーミングサーバ60は、送信側VPN50に接続し、送信側VPN50、ルータ40、提供側VPN20を介して、情報提供部10に要求データや情報提供部10に対する指示を含む指示データ等を送信する。又、ストリーミングサーバ60は、携帯端末70と無線リンクを確立し、情報提供部10から取得した映像データをストリーミング方式により携帯端末70に送信する。

**【0027】**

又、ストリーミングサーバ60は、携帯端末70のユーザの認証処理を行う。このように、ストリーミングサーバ60が、情報提供部10に代わって、携帯端末70のユーザが、情報提供者から映像データの受信の許可を受けたユーザであるか否かを確認する。そして、ストリーミングサーバ60が、認証処理により映像データの受信の許可を受けたユーザであることが確認できた携帯端末70からの要求にだけ応じて、情報提供部10に要求データや指示データを送信する。その結果、映像提供部10は、受信の許可を受けたユーザが使用する携帯端末70にのみ映像データを提供することができる。

**【0028】**

送信側VPN50は、情報送信手段であるストリーミングサーバ60が接続するアクセス制限がされた情報提供側ネットワークである。送信側VPN50は、ルータ40に接続する。送信側VPN50は、ルータ40を介して提供側VPN20と接続する。送信側VPN50は、認証サーバ51を備える。認証サーバ51は、送信側VPN50にアクセスしようとするストリーミングサーバ60やそ



の他の端末に対して、ユーザIDやパスワード、発ID等を用いた認証を行って、アクセスを制限する。そのため、ストリーミングサーバ60も、最初に送信側VPN50にアクセスして接続を確立する際には認証処理を受ける。

#### 【0029】

ストリーミングサーバ60と、送信側VPN50は、同じセキュリティポリシーを持ち、同じ体系のアドレスを用いる。映像データ等の情報データを携帯端末70に送信するサービスを行う情報送信者により、独自のセキュリティポリシー、独自のアドレス体系で統一された送信側VPN50と、ストリーミングサーバ60とが構築される。

#### 【0030】

ルータ40は、情報送信側ネットワークである送信側VPN50と情報提供側ネットワークである提供側VPN20とを接続する。そして、ルータ40は、送信側VPN50を介して受信したデータがストリーミングサーバ60から送信されたデータであるか否か、提供側VPN20を介して受信したデータが映像提供部10から送信されたデータであるか否かを判断し、その判断結果に基づいて、送信側VPN50を介して受信したデータ及び提供側VPN20を介して受信したデータの転送を行う転送手段である。尚、ルータ40とは、ルーティング機能を備えるものをいう。

#### 【0031】

携帯端末70は、ストリーミングサーバ60と無線リンクを確立して、映像データを受信する。携帯端末70は、ストリーミングサーバ60に対して、必要な映像データの種類やカメラ11の設置場所を指定して映像データの要求を行ったり、撮影する対象の切り替えや角度の変更等の指示を行ったりして、所望の映像データを受信する。携帯端末70は、受信した符号化された映像データをデコードして再生する。

#### 【0032】

次に、各構成について詳細に説明する。まず、ルータ40について詳細に説明する。図2に示すように、ルータ40は、インタフェース（以下「I/F」とする）41、42と、制御部43と、テーブル44とを備える。I/F41は、送

信側VPN50と接続する。又、I/F42は、提供側VPN20と接続する。このように、ルータ40は、送信側VPN50に接続するI/F41と提供側VPN20に接続するI/F42とを備えることにより、送信側VPN50と提供側VPN20とを接続する。I/F41は、送信側VPN50を介してデータを受信し、受信したデータを制御部43に入力する。又、I/F41は、制御部43から入力されたデータを、送信側VPN50を介してストリーミングサーバ60に転送する。一方、I/F42は、提供側VPN20を介してデータを受信し、受信したデータを制御部43に入力する。又、I/F42は、制御部43から入力されたデータを提供側VPN20を介して、映像提供部10に転送する。

### 【0033】

制御部43は、データ転送の制御を行う。まず、制御部43は、送信側VPN50を介して受信したデータがストリーミングサーバ60から送信されたデータであるか否かと、提供側VPN20を介して受信したデータが情報提供部10から送信されたデータであるか否かを判断し、その判断結果に基づいてデータ転送の制御を行う。その際、ルータ40は、ストリーミングサーバ60から情報提供部10に送信されたデータに付加されているアドレスを、提供側VPN20に適したアドレス（以下「提供側VPNアドレス」という）に変換し、情報提供部10からストリーミングサーバ60に送信されたデータに付加されているアドレスを、送信側VPN50に適したアドレス（以下「送信側VPNアドレス」という）に変換してデータ転送を行う。尚、提供側VPNアドレスや送信側VPNアドレスとしては、例えば、それぞれのネットワークで設定したローカルアドレス等を用いることができる。このように、データにはアドレスが付加されている。

### 【0034】

ここで、テーブル44は、各情報提供部10に付与されているアドレスと、ストリーミングサーバ60に付与されているアドレスを保持する。更に、テーブル44は、各情報提供部10に付与されている提供側VPNアドレスに対応する送信側VPNアドレスも保持する。同様に、テーブル44は、ストリーミングサーバ60に付与されている送信側VPNアドレスに対応する提供側VPNアドレスも保持する。図3に、ある情報提供部10に提供側VPNアドレスで「abcd

」というアドレスが付与されており、それに対応する送信側VPNアドレスが「ABCD」であり、ストリーミングサーバ60に送信側VPNアドレスで、「EFGH」というアドレスが付与されており、それに対応する提供側VPNアドレスが「efgh」である場合のテーブル44を示す。

#### 【0035】

制御部43は、I/F41から、送信側VPN50を介してルータ40が受信したデータを入力されると、テーブル44を参照して、データに付加されている送信元アドレスが、テーブル44が保持するストリーミングサーバ60のアドレスと一致するか否かを判断する。例えば、ルータ40が、送信側VPN50を介して、図3(a)に示すような要求データに、送信元アドレスと、あて先アドレスとが付加されているパケット101を受信したとする。この場合、制御部43は、パケット101の送信元アドレス「EFGH」がテーブル44に保持されたストリーミングサーバ60の送信側VPNアドレスと一致するため、要求データがストリーミングサーバ60から送信されたデータであると判断する。

#### 【0036】

次に、制御部43は、テーブル44を参照して、パケット101の送信側VPNアドレスで示された送信元アドレス及びあて先アドレスに対応する提供側VPNアドレスを取得する。制御部43は、パケット101の送信側VPNアドレスで示された送信元アドレス「EFGH」及びあて先アドレス「ABCD」を、取得した提供側VPNアドレスで示された送信元アドレス「efgh」及びあて先アドレス「abcd」に変換し、図3(b)に示すパケット102を得る。最後に、制御部43は、アドレスを変換したパケット102をI/F42に入力し、パケット102を提供側VPN20を介して情報提供部10に転送する。

#### 【0037】

同様に、制御部43は、I/F42から、提供側VPN20を介してルータ40が受信したデータを入力されると、テーブル44を参照して、データに付加されている送信元アドレスが、テーブル44が保持する情報提供部10のアドレスの中にあるか否かを判断する。例えば、ルータ40が、提供側VPN20を介して、図3(c)に示すような映像データに、送信元アドレスと、あて先アドレス

とが付加されたパケット103を受信したとする。この場合、制御部43は、パケット103の送信元アドレス「a b c d」が、テーブル44に保持された情報提供部10の提供側VPNアドレスと一致するため、映像データが情報提供部10から送信されたデータであると判断する。

#### 【0038】

次に、制御部43は、テーブル44を参照して、パケット103の提供側VPNアドレスで示された送信元アドレス及びあて先アドレスに対応する送信側VPNアドレスを取得する。制御部43は、パケット103の提供側VPNアドレスで示された送信元アドレス「a b c d」及びあて先アドレス「e f g h」を、取得した送信側VPNアドレスで示された送信元アドレス「A B C D」及びあて先アドレス「E F G H」に変換し、図3（d）に示すパケット104を得る。最後に、制御部43は、変換したパケット104をI/F41に入力し、パケット104を送信側VPN50を介してストリーミングサーバ60に転送する。

#### 【0039】

尚、制御部43は、送信側VPN50を介してルータ40が受信したデータに付加されている送信元アドレスが、テーブル44が保持するストリーミングサーバ60の送信側VPNアドレスと一致しない場合、そのデータを転送せずに破棄する。同様に、制御部43は、提供側VPN20を介してルータ40が受信したデータに付加されている送信元アドレスが、テーブル44が保持する情報提供部10の提供側VPNアドレスの中に含まれていない場合、そのデータを転送せずに破棄する。

#### 【0040】

更に、制御部43は、情報提供部10からの映像データを同時に転送するデータ量の閾値を保持している。データ量の閾値は、提供側VPN20、送信側VPN50、ルータ40、ストリーミングサーバ60の処理能力、ストリーミングサーバ60が携帯端末70に映像データを送信する際の品質、ストリーミングサーバ60と無線リンクを確立し、映像データの受信を行っている携帯端末70の数等に応じて設定することができる。尚、映像データを同時に転送するデータ量は、例えば、単位時間あたりに転送するデータ量、即ち、転送の速度等を用いて表

することができる。

#### 【0041】

制御部43は、提供側VPN20を介してルータ40が受信した映像提供部10から送信された映像データのデータ量と閾値とを比較する。尚、ルータ40が受信した映像データのデータ量も、例えば、ルータ40が単位時間当たり受信するデータ量、即ち、提供側VPN20のデータ伝送速度等を用いて表すことができる。そして、制御部43は、その比較結果に基づいてデータの転送を制御する。具体的には、制御部43は、提供側VPN20を介してルータ40が受信している映像データのデータ量が閾値未満の場合には、現在、映像データの提供を行っていない新たな情報提供部10に対するストリーミングサーバ60からの要求データを受信した場合に、その要求データの転送を行う。

#### 【0042】

一方、制御部43は、提供側VPN20を介してルータ40が受信した映像データのデータ量が閾値以上となった場合には、現在、映像データの提供を行っていない新たな情報提供部10に対するストリーミングサーバ60からの要求データを受信した場合に、その要求データの転送を行わない。更に、制御部43は、ストリーミングサーバ60に対して、要求データの転送を拒否する通知を行う。具体的には、制御部43は、転送拒否の通知をI/F41に入力する。そして、I/F41が、送信側VPN50を介して転送拒否の通知をストリーミングサーバ60に送信する。このようにして、ルータ40が、情報提供部10からの映像データを同時に転送するデータ量が閾値に達すると、ストリーミングサーバ60からの新たな映像データの要求を拒否することにより、余計な要求データの転送を回避することができる。

#### 【0043】

尚、このようなルータ40は、コンピュータに、情報送信側ネットワークと情報提供側ネットワークとを接続し、情報送信側ネットワークを介して受信したデータが情報送信手段から送信されたデータであるか否か及び情報提供側ネットワークを介して受信したデータが情報提供手段から送信されたデータであるか否かを判断し、その判断結果に基づいて、情報送信側ネットワークを介して受信した

データ及び情報提供側ネットワークを介して受信したデータの転送を行う転送手段として機能させるためのプログラムを実行させることにより実現できる。

#### 【0044】

次に、ストリーミングサーバ60について詳細に説明する。図4に示すように、ストリーミングサーバ60は、I/F61、62と、制御部63と、データベース64と、送信部65とを備える。I/F61は、携帯端末70と無線リンクを確立してデータのやりとりを行う。I/F61は、携帯端末70から、認証処理におけるユーザIDやパスワード、発ID、必要な映像データの種別を指定した映像データの要求や、撮影する対象の切り替えや角度の変更の指示等を受信する。I/F61は、携帯端末70から受信したユーザIDやパスワード、発ID、要求や指示を制御部63に入力する。又、I/F61には、送信部65から映像データが入力される。又、I/F61には、制御部63からストリーミングサーバ60から携帯端末70に対する指示や通知等の制御データが入力される。I/F61は、入力された映像データや制御データを、無線リンクを介して携帯端末70に送信する。

#### 【0045】

I/F62は、送信側VPN50と接続する。I/F62は、送信側VPN50を介して、情報提供部10からの映像データを受信して取得する。又、I/F62は、送信側VPN50を介して、ルータ40からの転送拒否の通知等を受信する。I/F62は、受信した映像データや転送拒否の通知を制御部63に入力する。又、I/F62は、制御部63から要求データや指示データを含むパケットを入力される。I/F62は、入力された要求データや指示データを含むパケットを、送信側VPN50を介して情報提供部10に送信する。

#### 【0046】

データベース64は、情報提供者が携帯端末70のユーザに付与したユーザIDやパスワード、発ID等のユーザに関する情報を保持する。又、データベース64は、各情報提供部10が提供する映像データの種別や映像提供部10の設置場所、各映像提供部10に付与されているアドレスを送信側VPNアドレスで示したもの等の映像提供部10に関する情報を保持する。又、データベース64は

、要求データや指示データを送信して映像データを取得する際に用いる制御情報等も保持する。

#### 【0047】

制御部63は、映像提供部10に対する要求データや指示データの送信を制御する。又、制御部63は、取得した映像データの携帯端末70への送信を制御する。又、制御部63は、携帯端末70のユーザの認証処理も行う。

#### 【0048】

まず、制御部63は、携帯端末70からの映像データの要求をI/F61から入力されると、携帯端末70にユーザIDやパスワード、発IDの入力を要求し、認証処理を行う。具体的には、制御部63は、携帯端末70からのユーザIDやパスワード、発IDをI/F61から入力されると、データベース64を参照して、ユーザIDやパスワード、発IDがデータベース64に保持されているものと一致するか否かを判断する。制御部63は、ユーザIDやパスワード、発IDが一致しない場合には、携帯端末70に再度、ユーザIDやパスワード、発IDの入力を要求する。そして、制御部63は、所定回数の認証を行っても、ユーザIDやパスワード、発IDがデータベース64に保持されているものと一致しない場合には、その携帯端末70からの映像データの要求を拒否する。

#### 【0049】

制御部63は、ユーザIDやパスワード、発IDが一致し、携帯端末70のユーザが映像データの受信の許可を受けたユーザであることが確認できた場合には、データベース64を参照して、携帯端末70が要求する種類や場所の映像データを提供している情報提供部10の送信側VPNアドレスで示されたアドレスを取得する。そして、制御部63は、あて先アドレスに送信側VPNアドレスで示された情報提供部10のアドレスを設定し、送信元アドレスに送信側VPNアドレスで示されたストリーミングサーバ60のアドレスを設定し、映像データの種類や場所を指定した映像データを要求する要求データを含む図3(a)に示すようなパケット101を生成する。制御部63は、生成したパケット101をI/F62に入力して、情報提供部10に送信するよう指示する。又、制御部63は、I/F61から、一度、認証処理を行った携帯端末70からの指示を入力され

ると、要求データを含むパケットを生成する場合と同様にして、情報提供部10に送信する指示データを含むパケットを生成し、I/F62に入力する。このようにして、制御部63は、映像提供部10に対して映像データの提供を要求したり、指示をしたりする。

#### 【0050】

制御部63は、要求データや指示データを情報提供部10に送信するときに、その要求データや指示データにシーケンス番号を付与する。制御部63は、要求データや指示データに付与したシーケンス番号と、その要求や指示をストリーミングサーバ60に対して行った携帯端末70のアドレスとを対応付けた制御情報をデータベース64に記録しておく。

#### 【0051】

制御部63は、I/F62から映像提供部10から取得した映像データを入力される。映像データには、その映像データを取得するために送信した要求データや指示データのシーケンス番号と同じシーケンス番号が付与されている。制御部63は、映像データに付与されているシーケンス番号に基づいてデータベース64を参照し、その映像データに対する要求や指示を行った携帯端末70のアドレスを取得する。そして、制御部63は、取得した映像データに携帯端末70のアドレスを付加して送信部65に入力し、携帯端末70に送信するよう指示する。送信部65は、制御部63から入力された映像データを、I/F61を介して携帯端末70に送信する。送信部65は、ストリーミング方式により映像データを送信する。尚、制御部63は、I/F62がルータ40からの転送拒否の通知を受信した場合には、携帯端末70に対して、現在、ネットワークが混雑していて映像データの提供ができないことを通知する混雑通知を生成する。制御部63は、生成した混雑通知をI/F61に入力する。そして、I/F61が、混雑通知を携帯端末70に送信する。

#### 【0052】

次に、映像提供部10について詳細に説明する。図5に示すように、映像提供部10は、カメラ11と映像提供サーバ12とを備える。カメラ11は、映像を撮影する撮影手段である。カメラ11は、映像提供サーバ12から入力される指



示に応じて動作する。例えば、カメラ 11 は、映像提供サーバ 12 により、撮影した映像データの入力や撮影する対象の切り替え、角度の変更等の指示を受ける。カメラ 11 は、映像提供サーバ 12 からの指示に従い撮影し、リアルタイムで撮影している映像データを映像提供サーバ 12 に入力する。

#### 【0053】

映像提供サーバ 12 は、ストリーミングサーバ 60 からの要求データや指示データに基づいてカメラ 11 を制御し、カメラ 11 が撮影した映像データをストリーミングサーバ 60 に提供する。映像提供サーバ 12 は、I/F 121、122 と、制御部 123 と、エンコーダ 124 とを備える。I/F 121 は、提供側 VPN 20 と接続する。I/F 211 は、提供側 VPN 20 を介して、ストリーミングサーバ 60 から要求データや指示データを受信する。I/F 121 は、受信した要求データや指示データを制御部 123 に入力する。又、I/F 121 には、制御部 123 から映像データが入力される。I/F 121 は、制御部 123 から入力された映像データを、提供側 VPN 20 を介してストリーミングサーバ 60 に送信する。

#### 【0054】

又、I/F 122 は、カメラ 11 と接続している。I/F 122 は、制御部 123 から入力される指示をカメラ 11 に入力する。又、I/F 122 は、カメラ 11 から入力された映像データをエンコーダ 124 に入力する。エンコーダ 124 は、I/F 122 から入力された映像データを符号化する。エンコーダ 124 は、符号化した映像データを制御部 123 に入力する。

#### 【0055】

制御部 123 は、I/F 121 から入力された要求データや指示データに基づいて、カメラ 11 に指示をしてカメラ 11 を制御する。制御部 123 は、カメラ 11 に対する指示を、I/F 122 に入力する。又、制御部 123 は、エンコーダ 124 から入力された映像データに、その映像データに関する要求データや指示データに付与されていたシーケンス番号と同じシーケンス番号を付与する。又、制御部 123 は、提供側 VPN アドレスで示されたストリーミングサーバ 60 のアドレスを保持する。そして、制御部 63 は、あて先アドレスに提供側 VPN

アドレスで示されたストリーミングサーバ60のアドレスを設定し、送信元アドレスに提供側VPNアドレスで示された映像提供部10のアドレスを設定し、映像データを含む図3(c)に示すようなパケット103を生成する。制御部63は、生成したパケット103をI/F121に入力して、ストリーミングサーバ60に送信するよう指示する

(通信方法)

次に、図1に示す通信システム1を用いて行う通信方法について説明する。図6に示すように、まず、携帯端末70が、ストリーミングサーバ60に対して映像データを要求する(S101)。ストリーミングサーバ60は、携帯端末70に対してユーザIDやパスワード、発IDの入力を要求し、認証処理を行う(S102)。ストリーミングサーバ60は、認証処理の結果、携帯端末70のユーザが情報提供者により受信を許可されたユーザであると判断すると、携帯端末70からの要求に基づく要求データを含むパケットを映像提供部10に対して送信する(S103)。このとき、要求データには、送信側VPNアドレスで示されたアドレスが付与される。

【0056】

ルータ40は、送信側VPN50を介してストリーミングサーバ60からの要求データを含むパケットを受信する。ルータ40は、要求データに付与されている送信側VPNアドレスで示されたアドレスを、提供側VPNアドレスで示されたアドレスに変換する(S104)。そして、ルータ40は、提供側VPNアドレスで示されたアドレスが付与された要求データを含むパケットを、映像提供部10に転送する(S105)。映像提供部10は、受信した要求データに応じた映像データをストリーミングサーバ60に対して送信する(S106)。このとき、映像データには、提供側VPNアドレスで示されたアドレスが付与される。

【0057】

ルータ40は、提供側VPN20を介し映像提供部10からの映像データを含むパケットを受信する。ルータ40は、映像データに付与されている提供側VPNアドレスで示されたアドレスを、送信側VPNアドレスで示されたアドレスに変換する(S107)。そして、ルータ40は、送信側VPNアドレスで示され

たアドレスが付与された映像データを含むパケットを、ストリーミングサーバ60に転送する(S108)。ストリーミングサーバ60は、映像提供部10から取得した映像データを携帯端末70に送信する(S109)。

#### 【0058】

(効果)

このような本実施形態に係る通信システム1、ルータ40及び通信方法によれば、映像提供部10はアクセス制限がされた提供側VPN20に接続し、ストリーミングサーバ60は、アクセス制限がされた送信側VPN50に接続して、映像提供部10とストリーミングサーバ60は、それぞれ異なるネットワークに接続する。そして、ルータ40は、送信側VPN50を介して受信した要求データや指示データがストリーミングサーバ60から送信されたデータであるか否かを判断し、提供側VPNを介して受信した映像データが情報提供部10から送信されたデータであるか否かを判断し、それらの判断結果に基づいて、送信側VPN50を介して受信したデータや提供側VPN20を介して受信したデータの転送を行う。

#### 【0059】

そのため、ストリーミングサーバ60と情報提供部10が両方とも接続するような、セキュリティポリシーの統一された1つのネットワークを構築する必要がない。よって、ストリーミングサーバ60及び送信側VPN50と、情報提供部10及び提供側VPN20は、それぞれ独自のセキュリティポリシーを保ったまま、ルータ40を介して接続することができる。又、ルータ40が、送信側VPN50や提供側VPN20を介して受信したデータが、それぞれストリーミングサーバ60や情報提供部10から送信されたデータであるか否かを判断し、その判断結果に基づいてデータの転送を行う。

#### 【0060】

よって、ストリーミングサーバ60及び送信側VPN50と、情報提供部10及び提供側VPN20との間では、ストリーミングサーバ60又は情報提供部10から送信されたデータという特定のデータのみがやりとりされる。更に、提供側VPN20、送信側VPN50はそれぞれアクセス制限がされている。これら

の結果、通信システム 1 は、高いセキュリティを確保できる。

#### 【0061】

又、ストリーミングサーバ 60 と情報提供部 10 が両方とも接続するような、セキュリティポリシーの統一された 1 つのネットワークを構築する必要がない結果、ストリーミングサーバ 60 が接続する送信側 VPN 50 や情報提供部 10 が接続する提供側 VPN 20 として既存のものがあれば、それらをそのまま利用して通信システム 1 を構築して、映像提供サービスを行うことができる。よって、低コストで効率的に通信システム 1 を構築することができる。

#### 【0062】

又、通信システム 1 では、ストリーミングサーバ 60 及び送信側 VPN 50 と、情報提供部 10 及び提供側 VPN 20 との間では、ストリーミングサーバ 60 又は情報提供部 10 から送信されたデータという特定のデータのみがやりとりされる。そのため、ストリーミングサーバ 60 は、映像データのように容量の大きいデータであっても、効率よく受信することができる。

#### 【0063】

又、ルータ 40 は、ストリーミングサーバ 60 から情報提供部 10 に送信されたデータに付加されているアドレスを、提供側 VPN アドレスに変換し、情報提供部 10 からストリーミングサーバ 60 に送信された映像データに付加されているアドレスを、送信側 VPN アドレスに変換する。そのため、ストリーミングサーバ 60 及び送信側 VPN 50 と、情報提供部 10 及び提供側 VPN 20 は、それぞれ独自のアドレス体系を保ったまま、ルータ 40 を介して接続することができる。その結果、通信システム 1 はアドレス体系の統一を行う必要がなく、より低コストで通信システム 1 を構築することができる。又、情報提供部 10 は、独自のアドレスを利用して、映像データの提供サービスを行うことができる。

#### 【0064】

更に、ルータ 40 は、情報提供部 10 からの映像データを同時に転送するデータ量の閾値を保持し、提供側 VPN 20 を介して受信した情報提供部 10 から送信された映像データのデータ量と閾値を比較し、その比較結果に基づいてデータの転送を制御する。又、同時に転送するデータ量の閾値は、提供側 VPN 20、

送信側VPN50、ルータ40、ストリーミングサーバ60の処理能力、ストリーミングサーバ60が携帯端末70に映像データを送信する際の品質、ストリーミングサーバ60と無線リンクを確立し、映像データの受信を行っている携帯端末70の数等に応じて定めることができる。そのため、ルータ40は、提供側VPN20、送信側VPN50、ルータ40、ストリーミングサーバ60の処理能力、ストリーミングサーバ60が携帯端末70に映像データを送信する際の品質、映像データの受信を行っている携帯端末70の数等に応じた適切なデータの転送を行うことができる。

#### 【0065】

##### 〔第2の実施の形態〕

次に、本発明に係る第2の実施の形態について説明する。図7に示すように、本実施形態の通信システム201は、複数の映像提供部(A)10aと、提供側VPN(A)20aと、提供側サーバ(A)30aと、複数の映像提供部(B)10bと、提供側VPN(B)20bと、提供側サーバ(B)30bと、ルータ240と、送信側VPN50と、ストリーミングサーバ260と、複数の携帯端末(A)70aと、複数の携帯端末(B)70bとを備えている。送信側VPN50は、図1に示す送信側VPN50と実質的に同様であるため、同一の符号を付して説明を省略する。

#### 【0066】

映像提供部(A)10aは、カメラ(A)11aと映像提供サーバ(A)12aとを備える。映像提供部(A)10aは、提供側VPN(A)20aに接続する。そして、映像提供部(A)10aは、提供側VPN(A)20a、ルータ240、送信側VPN50を介して、ストリーミングサーバ260に映像データを送信する。映像提供部(A)10aは、情報提供者Aから、映像データの受信の許可を受けたユーザが使用する携帯端末(A)70aにのみ映像データを提供する。尚、携帯端末(A)70aは、映像データを受信するために、情報提供者Aから映像データの受信の許可を受けて、ユーザIDやパスワード、発IDを取得したユーザが使用する携帯端末である。

#### 【0067】

提供側VPN(A)20aは、映像提供部(A)10aが接続するアクセス制限がされた情報提供側ネットワークである。提供側VPN(A)20aは、ルータ240に接続し、ルータ240を介して送信側VPN50と接続する。提供側VPN(A)20aは、認証サーバ(A)21aを備える。認証サーバ(A)21aは、提供側VPN(A)20aにアクセスしようとする映像提供部(A)10a、提供側サーバ(A)30a、その他の端末に対して、ユーザIDやパスワード、発ID等を用いた認証を行って、アクセスを制限する。提供側サーバ(A)30aは、提供側VPN(A)20aに接続するサーバである。提供側サーバ(A)30aは、様々な情報処理を行う。

#### 【0068】

情報提供部(A)10aと、提供側VPN(A)20aと、提供側サーバ(A)30aは、同じセキュリティポリシーを持ち、同じ体系のアドレスを用いる。情報提供者Aにより、独自のセキュリティポリシー、独自のアドレス体系で統一された情報提供部(A)10aと、提供側VPN(A)20aと、提供側サーバ(A)30aとが構築される。

#### 【0069】

又、映像提供部(B)10bは、カメラ(B)11bと映像提供サーバ(B)12bとを備える。映像提供部(B)10bは、提供側VPN(B)20bに接続する。そして、映像提供部(B)10bは、提供側VPN(B)20b、ルータ240、送信側VPN50を介して、ストリーミングサーバ260に映像データを送信する。映像提供部(B)10bは、情報提供者Bから、映像データの受信の許可を受けたユーザが使用する携帯端末(B)70bにのみ映像データを提供する。尚、携帯端末(B)70bは、映像データを受信するために、情報提供者Bから映像データの受信の許可を受けて、ユーザIDやパスワード、発IDを取得したユーザが使用する携帯端末である。

#### 【0070】

提供側VPN(B)20bは、映像提供部(B)10bが接続するアクセス制限がされた情報提供側ネットワークである。提供側VPN(B)20bは、ルータ240に接続し、ルータ240を介して送信側VPN50と接続する。提供側

VPN (B) 20b は、認証サーバ (B) 21b を備える。認証サーバ (B) 21b は、提供側 VPN (B) 20b にアクセスしようとする映像提供部 (B) 10b、提供側サーバ (B) 30b、その他の端末に対して、ユーザ ID やパスワード、発 ID 等を用いた認証を行って、アクセスを制限する。提供側サーバ (B) 30b は、提供側 VPN (B) 20b に接続するサーバである。提供側サーバ (B) 30b は、様々な情報処理を行う。

#### 【0071】

情報提供部 (B) 10b と、提供側 VPN (B) 20b と、提供側サーバ (B) 30b は、同じセキュリティポリシーを持ち、同じ体系のアドレスを用いる。情報提供者 A と異なる情報提供者 B により、独自のセキュリティポリシー、独自のアドレス体系で統一された情報提供部 (B) 10b と、提供側 VPN (B) 20b と、提供側サーバ (B) 30b とが構築される。

#### 【0072】

このように、通信システム 201 は、提供側 VPN (A) 20a や提供側 VPN (B) 20b のような情報提供側ネットワークを複数備える。そして、複数の情報提供側ネットワークである提供側 VPN (A) 20a や提供側 VPN (B) 20b に、それぞれ情報提供部 (A) 10a や情報提供部 (B) 10b が接続する。具体的には、上記したように、提供側 VPN (A) 20a には、同じセキュリティポリシーを持ち、同じ体系のアドレスを用いる複数の情報提供部 (A) 10a が接続する。又、提供側 VPN (B) 20b には、同じセキュリティポリシーを持ち、同じ体系のアドレスを用いる複数の情報提供部 (B) 10b が接続する。このように、通信システム 201 には、情報提供部からストリーミングサーバ 260 までのセキュリティを確保したいグループとして、情報提供部 (A) 10a からストリーミングサーバ 260 までのグループと、情報提供部 (B) 10b からストリーミングサーバ 260 までのグループという複数のグループが存在する。

#### 【0073】

ストリーミングサーバ 260 は、携帯端末から映像提供部 (A) 10a に対する要求や指示を受けた場合には、携帯端末のユーザが情報提供者 A により映像デ

ータの受信の許可を受けたユーザであるか否かを確認する認証処理を行う。そして、ストリーミングサーバ260は、情報提供者Aにより映像データの受信の許可を受けたユーザであることが確認できた携帯端末(A)70aからの要求にだけ応じて、情報提供部(A)10aに要求データや指示データを送信する。そして、ストリーミングサーバ260は、映像提供部(A)10aに対して要求データや指示データを送信して取得した映像データを、携帯端末(A)70aに送信する。

#### 【0074】

同様に、ストリーミングサーバ260は、携帯端末から映像提供部(B)10bに対する要求や指示を受けた場合には、携帯端末のユーザが情報提供者Bにより映像データの受信の許可を受けたユーザであるか否かを確認する認証処理を行う。そして、ストリーミングサーバ260は、情報提供者Bにより映像データの受信の許可を受けたユーザであることが確認できた携帯端末(B)70bからの要求にだけ応じて、情報提供部(B)10bに要求データや指示データを送信する。そして、ストリーミングサーバ260は、映像提供部(B)10bに対して要求データや指示データを送信して取得した映像データを、携帯端末(B)70bに送信する。

#### 【0075】

これにより、映像提供部(A)10aは、映像提供者Aにより許可を受けたユーザが使用する携帯端末(A)70aにのみ映像データを提供することができ、映像提供部(B)10bは、映像提供者Bにより許可を受けたユーザが使用する携帯端末(B)70bにのみ映像データを提供することができる。これらの点以外は、ストリーミングサーバ260は、図1、図4に示したストリーミングサーバ60と実質的に同様である。

#### 【0076】

ルータ240は、図8に示すように、I/F241、242a、242bと、制御部243と、データベース244とを備える。I/F241は、送信側VPN50と接続する。又、I/F242aは、提供側VPN(A)20aと接続する。更に、I/F242bは、提供側VPN(B)20bと接続する。このよう



に、ルータ240は、送信側VPN50に接続するI/F241と、提供側VPN(A)20aに接続するI/F242aと、提供側VPN(B)20bに接続するI/F242bとを備えることにより、送信側VPN50と、提供側VPN(A)20a及び提供側VPN(B)20bとを接続する。即ち、ルータ240は、複数ある情報提供側ネットワークの数だけ情報提供側ネットワークと接続するI/Fを備えることにより、情報送信側ネットワークと、複数の情報提供側ネットワークとを接続することができる。尚、ルータ240とは、ルーティング機能を備えるものをいう。

#### 【0077】

I/F241は、図2に示すI/F41と実質的に同様である。一方、I/F242aは、VPN(A)20aを介してデータを受信し、受信したデータを制御部243に入力する。又、I/F242aは、制御部243から入力されたデータを、提供側VPN(A)20aを介して映像提供部(A)10aに転送する。又、I/F242bは、提供側VPN(B)20bを介してデータを受信し、受信したデータを制御部243に入力する。又、I/F242bは、制御部243から入力されたデータを、VPN(B)20bを介して映像提供部(B)10bに転送する。

#### 【0078】

制御部243は、送信側VPN50を介して受信したデータがストリーミングサーバ260から送信されたデータであるか否かと、提供側VPN(A)20aや提供側VPN(B)20bを介して受信したデータが情報提供部(A)10aや情報提供部(B)10bから送信されたデータであるか否かを判断し、その判断結果に基づいてデータ転送の制御を行う。

#### 【0079】

その際、ルータ240は、ストリーミングサーバ260から情報提供部(A)10aに対して送信されたデータに付加されているアドレスを、提供側VPN(A)20aに適したアドレス（以下「提供側VPN(A)アドレス」という）に変換し、ストリーミングサーバ260から情報提供部(B)10bに対して送信されたデータに付加されているアドレスを、提供側VPN(B)20bに適した

アドレス（以下「提供側VPN（B）アドレス」という）に変換し、情報提供部（A）10aや情報提供部（B）10bからストリーミングサーバ260に対して送信されたデータに付加されているアドレスを送信側VPNアドレスに変換してデータ転送を行う。

#### 【0080】

ここで、データベース244は、テーブル244aと、テーブル244bとを備える。テーブル244aは、各情報提供部（A）10aに付与されているアドレスと、ストリーミングサーバ260に付与されているアドレスを保持する。更に、テーブル244aは、各情報提供部（A）10aに付与されている提供側VPN（A）アドレスに対応する送信側VPNアドレスも保持する。同様に、テーブル244aは、ストリーミングサーバ260に付与されている送信側VPNアドレスに対応する提供側VPN（A）アドレスも保持する。図8に、ある情報提供部（A）10aに提供側VPN（A）アドレスで「abcd」というアドレスが付与されており、それに対応する送信側VPNアドレスが「ABCD」であり、ストリーミングサーバ260に送信側VPNアドレスで、「EFGH」というアドレスが付与されており、それに対応する提供側VPN（A）アドレスが「efgh」である場合のテーブル244aを示す。

#### 【0081】

一方、テーブル244bは、各情報提供部（B）10bに付与されているアドレスと、ストリーミングサーバ260に付与されているアドレスを保持する。更に、テーブル244bは、各情報提供部（B）10bに付与されている提供側VPN（B）アドレスに対応する送信側VPNアドレスも保持する。同様に、テーブル244bは、ストリーミングサーバ260に付与されている送信側VPNアドレスに対応する提供側VPN（B）アドレスも保持する。図8に、ある情報提供部（B）10bに提供側VPN（B）アドレスで「1234」というアドレスが付与されており、それに対応する送信側VPNアドレスが「IJKL」であり、ストリーミングサーバ260に送信側VPNアドレスで、「EFGH」というアドレスが付与されており、それに対応する提供側VPN（B）アドレスが「5678」である場合のテーブル244bを示す。

## 【0082】

制御部243は、I/F241から、送信側VPN50を介してルータ240が受信したデータを入力されると、テーブル244a, 244bを参照して、データに付加されている送信元アドレスが、テーブル244a, 244bが保持するストリーミングサーバ260のアドレスと一致するか否かを判断する。図8の場合、制御部243は、送信元アドレスがテーブル244a, 244bに保持されたストリーミングサーバ260の送信側VPNアドレス「EFGH」と一致する場合、要求データや指示データがストリーミングサーバ260から送信されたデータであると判断する。

## 【0083】

次に、制御部243は、テーブル244a, 244bを参照して、送信側VPNアドレスで示されたあて先アドレスを検索する。ここで、あて先アドレスが「ABCD」であり、テーブル244aに保持された送信側VPNアドレスと一致する場合、制御部243は、テーブル244aから、送信側VPNアドレスで示された送信元アドレス「EFGH」及びあて先アドレス「ABCD」に対応する提供側VPN(A)アドレスを取得する。

## 【0084】

制御部243は、送信側VPNアドレスで示された送信元アドレス「EFGH」を、取得した提供側VPN(A)アドレス「efgh」に、送信側VPNアドレスで示されたあて先アドレス「ABCD」を、取得した提供側VPN(A)アドレス「abcd」に変換する。最後に、制御部243は、あて先アドレスが提供側VPN(A)アドレスで示された「abcd」であることから、受信した要求データや指示データは、情報提供部(A)10a宛ての要求データや指示データであると判断する。そして、制御部243は、送信元アドレスやあて先アドレスを変換した要求データや指示データを含むパケットを、I/F242aに入力し、パケットを提供側VPN(A)20aを介して情報提供部(A)10aに転送する。

## 【0085】

一方、あて先アドレスが「IJKL」であり、テーブル244bに保持された

送信側VPNアドレスと一致する場合、制御部243は、テーブル244bから、送信側VPNアドレスで示された送信元アドレス「EFGH」及びあて先アドレス「IJKL」に対応する提供側VPN(B)アドレスを取得する。

#### 【0086】

制御部243は、送信側VPNアドレスで示された送信元アドレス「EFGH」を、取得した提供側VPN(B)アドレス「5678」に、送信側VPNアドレスで示されたあて先アドレス「IJKL」を取得した提供側VPN(B)アドレス「1234」に変換する。最後に、制御部243は、あて先アドレスが提供側VPN(B)アドレスで示された「1234」であることから、受信した要求データや指示データは、情報提供部(B)10b宛ての要求データや指示データであると判断する。そして、制御部243は、送信元アドレスやあて先アドレスを変換した要求データや指示データを含むパケットを、I/F242bに入力し、パケットを提供側VPN(B)20bを介して情報提供部(B)10bに転送する。

#### 【0087】

又、制御部243は、I/F242aから、提供側VPN(A)20aを介してルータ240が受信した映像データを入力されると、テーブル244aを参照して、映像データに付加されている送信元アドレスが、テーブル244aが保持する情報提供部(A)10aのアドレスと一致するか否かを判断する。図8の場合、制御部243は、送信元アドレスがテーブル244aに保持された映像提供部(A)10aの提供側VPN(A)アドレス「abcd」と一致する場合、映像データが情報提供部(A)10aから送信された映像データであると判断する。

#### 【0088】

次に、制御部243は、テーブル244aを参照して、提供側VPN(A)アドレスで示された送信元アドレス「abcd」及びあて先アドレス「efgh」に対応する送信側VPNアドレスを取得する。制御部243は、提供側VPN(A)アドレスで示された送信元アドレス「abcd」を取得した送信側VPNアドレス「ABCD」に、提供側VPN(A)アドレスで示されたあて先アドレス

「e f g h」を取得した送信側VPNアドレス「E F G H」に変換する。最後に、制御部243は、送信元アドレスやあて先アドレスを変換した映像データを含むパケットを、I/F241に inputs し、パケットを送信側VPN50を介してストリーミングサーバ60に転送する。

#### 【0089】

一方、制御部243は、I/F242bから、提供側VPN(B)20bを介してルータ240が受信した映像データを入力されると、テーブル244bを参照して、映像データに付加されている送信元アドレスが、テーブル244bが保持する情報提供部(B)10bのアドレスと一致するか否かを判断する。図8の場合、制御部243は、送信元アドレスがテーブル244bに保持された映像提供部(B)10bの提供側VPN(B)アドレス「1234」と一致する場合、映像データが情報提供部(B)10bから送信された映像データであると判断する。

#### 【0090】

次に、制御部243は、テーブル244bを参照して、提供側VPN(B)アドレスで示された送信元アドレス「1234」及びあて先アドレス「5678」に対応する送信側VPNアドレスを取得する。制御部243は、提供側VPN(B)アドレスで示された送信元アドレス「1234」を取得した送信側VPNアドレス「I J K L」に、提供側VPN(B)アドレスで示されたあて先アドレス「5678」を取得した送信側VPNアドレス「E F G H」に変換する。最後に、制御部243は、送信元アドレスやあて先アドレスを変換した映像データを含むパケットを、I/F241に inputs し、パケットを送信側VPN50を介してストリーミングサーバ60に転送する。

#### 【0091】

尚、制御部243は、送信側VPN50を介してルータ240が受信したデータに付加されている送信元アドレスが、テーブル244a, 244bが保持する送信側VPNアドレスで示されたストリーミングサーバ60のアドレスと一致しない場合、そのデータを転送せずに破棄する。同様に、制御部243は、提供側VPN(A)20aや提供側VPN(B)20bを介してルータ240が受信し

たデータに付加されている送信元アドレスが、テーブル 244 a, 244 b が保持する提供側 VPN (A) アドレスや提供側 VPN (B) アドレスで示された情報提供部 (A) 10 a や情報提供部 (B) 10 b のアドレスの中に含まれていない場合、そのデータを転送せずに破棄する。

#### 【0092】

更に、制御部 243 は、情報提供部 (A) 10 a 及び情報提供部 (B) 10 b からの映像データを同時に転送するデータ量の閾値を保持している。データ量の閾値は、提供側 VPN (A) 20 a、提供側 VPN (B) 20 b、送信側 VPN 50、ルータ 240、ストリーミングサーバ 260 の処理能力、ストリーミングサーバ 260 が携帯端末 (A) 70 a や携帯端末 (B) 70 b に映像データを送信する際の品質、ストリーミングサーバ 260 と無線リンクを確立し、映像データの受信を行っている携帯端末 (A) 70 a 及び携帯端末 (B) 10 b の数等に応じて設定することができる。

#### 【0093】

制御部 243 は、情報提供側ネットワークを介してルータ 240 が受信した映像のデータ量、即ち、提供側 VPN (A) 20 a を介してルータ 240 が受信した映像データのデータ量と提供側 VPN (B) 20 b を介してルータ 240 が受信した映像データのデータ量の合計のデータ量と、閾値とを比較する。そして、制御部 243 は、提供側 VPN (A) 20 a を介してルータ 240 が受信している映像データのデータ量と提供側 VPN (B) 20 b を介してルータ 240 が受信している映像データのデータ量の合計のデータ量が閾値未満の場合には、現在、映像データの提供を行っていない新たな情報提供部 (A) 10 a や情報提供部 (B) 10 b に対するストリーミングサーバ 260 からの要求データを受信した場合に、その要求データの転送を行う。

#### 【0094】

一方、制御部 243 は、提供側 VPN (A) 20 a を介してルータ 240 が受信している映像データのデータ量と提供側 VPN (B) 20 b を介してルータ 240 が受信している映像データのデータ量の合計のデータ量が閾値以上となった場合には、現在、映像データの提供を行っていない新たな情報提供部 (A) 10

aや情報提供部(B)10bに対するストリーミングサーバ260からの要求データを受信した場合に、その要求データの転送を行わない。これらの点以外は、図2に示した制御部43と実質的に同様である。

#### 【0095】

このような本実施形態に係る通信システム201、や通信システム201を用いた通信方法によれば、図1に示す通信システム1や通信システム1を用いた通信方法による効果とほぼ同様の効果を得ることができる。加えて、通信システム201は、提供側VPN(A)20aと提供側VPN(B)20bという複数の情報提供側ネットワークを備え、その複数の情報提供側ネットワークである提供側VPN(A)20aと提供側VPN(B)20bにそれぞれ情報提供部(A)10a、情報提供部(B)10bが接続する。そして、ルータ240は、送信側VPN50と、提供側VPN(A)20a及び提供側VPN(B)20bとを接続する。

#### 【0096】

そのため、通信システム201は、ルータ240を介して、送信側VPN50と、複数の情報提供側ネットワークである提供側VPN(A)20a及び提供側VPN(B)20bとを接続することができる。よって、情報提供部からストリーミングサーバ260までのセキュリティを確保したいループが、情報提供部(A)10aからストリーミングサーバ260までと、情報提供部(B)10bからストリーミングサーバ260までのように多数存在する場合であっても、提供側VPN(A)20a、提供側VPN(B)20bのように情報提供側ネットワークをセキュリティを確保したいグループの数だけ設ければ、セキュリティを確保したいグループの数の送信側VPN50を設ける必要はない。例えば、図7に示すように、送信側VPN50、ルータ240及びストリーミングサーバ260は1つのままでよい。又、情報提供部とストリーミングサーバ260が両方とも接続するような1つのネットワークを、セキュリティを確保したいグループの数だけ設ける必要もない。よって、映像データを提供する情報提供側と情報送信側とが、独自のセキュリティポリシーを保つことができる通信システム201を、より低コストで構築することができる。

## 【0097】

## 〔第3の実施の形態〕

次に、本発明に係る第3の実施の形態について説明する。図9に示すように、本実施形態の通信システム301は、複数の映像提供部10と、提供側ATM（Asynchronous Transfer Mode：非同期転送モード）網320と、提供側サーバ30と、ルータ340と、送信側ATM網350と、ストリーミングサーバ60と、複数の携帯端末70とを備えている。映像提供部10と、提供側サーバ30と、ストリーミングサーバ60と、携帯端末70は、図1に示す映像提供部10と、提供側サーバ30と、ストリーミングサーバ60と、複数の携帯端末70と実質的に同様であるため、同一の符号を付して説明を省略する。

## 【0098】

提供側ATM網320は、映像提供部10が接続するアクセス制限がされた情報提供側ネットワークである。提供側ATM網320は、ルータ340に接続し、ルータ340を介して送信側ATM網350と接続する。提供側ATM網320は、認証サーバ321を備える。認証サーバ321は、提供側ATM網320にアクセスしようとする映像提供部10、提供側サーバ30、その他の端末に対して、ユーザIDやパスワード、発ID等を用いた認証を行って、アクセスを制限する。情報提供部10と、提供側ATM網320と、提供側サーバ30は、同じセキュリティポリシーを持ち、同じ体系のアドレスを用いる。情報提供者により、独自のセキュリティポリシー、独自のアドレス体系で統一された情報提供部10と、提供側ATM網320と、提供側サーバ30とが構築される。

## 【0099】

送信側ATM網350は、ストリーミングサーバ60が接続するアクセス制限がされた情報提供側ネットワークである。送信側ATM網350は、ルータ340に接続する。送信側ATM網350は、ルータ340を介して提供側ATM網320と接続する。送信側ATM網350は、認証サーバ351を備える。認証サーバ351は、送信側ATM網350にアクセスしようとするストリーミングサーバ60、その他の端末に対して、ユーザIDやパスワード、発ID等を用いた認証を行って、アクセスを制限する。ストリーミングサーバ60と、送信側A



TM網350は、同じセキュリティポリシーを持ち、同じ体系のアドレスを用いる。情報送信者により、独自のセキュリティポリシー、独自のアドレス体系で統一された送信側ATM網350と、ストリーミングサーバ60とが構築される。

#### 【0100】

ルータ340は、図10に示すように、I/F341、342と、制御部343と、データベース344とを備える。I/F341は、送信側ATM網350と接続する。又、I/F342は、提供側ATM網320と接続する。このように、ルータ340は、送信側ATM網350に接続するI/F341と提供側ATM網320に接続するI/F342とを備えることにより、送信側ATM網350と提供側ATM網320とを接続する。これらの点以外は、I/F341、342は、図2に示したI/F41、42と実質的に同様である。尚、ルータ340とは、ルーティング機能を備えるものをいう。

#### 【0101】

制御部343は、送信側ATM網350を介して受信したデータがストリーミングサーバ60から送信されたデータであるか否かと、提供側ATM網320を介して受信したデータが情報提供部10から送信されたデータであるか否かを判断し、その判断結果に基づいてデータ転送の制御を行う。その際、ルータ340は、ストリーミングサーバ60から情報提供部10に対して送信されたデータに付加されているアドレスや、情報提供部10からストリーミングサーバ60に対して送信されたデータに付加されているアドレスを、一度、提供側ATM網320に適したアドレス（以下「提供側ATMアドレス」という）及び送信側ATM網350に適したアドレス（以下「送信側ATMアドレス」という）以外のアドレス（以下「共通アドレス」という）に変換する。それから、制御部243は、変換した共通アドレスを、それぞれ送信側ATMアドレスや提供側ATMアドレスに変換して、データ転送を行う。

#### 【0102】

ここで、データベース344は、テーブル344aとテーブル344bとを備える。テーブル344a、344bは、各情報提供部10に付与されているアドレスと、ストリーミングサーバ60に付与されているアドレスを保持する。更に

、テーブル 3 4 4 a は、各情報提供部 1 0 やストリーミングサーバ 6 0 に付与されている提供側 A T M アドレスに対応する共通アドレスも保持する。同様に、テーブル 3 4 4 b は、ストリーミングサーバ 6 0 や各情報提供部 1 0 に付与されている送信側 A T M アドレスに対応する共通アドレスも保持する。

#### 【0 1 0 3】

図 1 0 に、ある情報提供部 1 0 に提供側 A T M アドレスで「a b c d」というアドレスが付与されており、それに対応する共通アドレスが「1 2 3 4」であり、ストリーミングサーバ 6 0 の共通アドレスが「5 6 7 8」であり、それに対応する提供側 A T M アドレスが「e f g h」である場合のテーブル 3 4 4 a を示す。又、図 1 0 に、ストリーミングサーバ 6 0 に送信側 A T M アドレスで「E F G H」というアドレスが付与されており、それに対応する共通アドレスが「5 6 7 8」であり、情報提供部 1 0 の共通アドレスが「1 2 3 4」であり、それに対応する送信側 A T M アドレスが「A B C D」である場合のテーブル 3 4 4 b を示す。

#### 【0 1 0 4】

制御部 3 4 3 は、I / F 3 4 1 から、送信側 A T M 網 3 5 0 を介してルータ 3 4 0 が受信した要求データや指示データを含むパケットを入力されると、テーブル 3 4 4 b を参照して、要求データや指示データに付加されている送信元アドレスが、テーブル 3 4 4 b が保持するストリーミングサーバ 6 0 の送信側 A T M アドレスと一致するか否かを判断する。図 1 0 の場合、制御部 3 4 3 は、送信元アドレスがテーブル 3 4 4 b に保持されたストリーミングサーバ 6 0 の送信側 A T M アドレス「E F G H」と一致する場合、要求データや指示データがストリーミングサーバ 6 0 から送信されたデータであると判断する。

#### 【0 1 0 5】

次に、制御部 3 4 3 は、テーブル 3 4 4 b を参照して、送信側 A T M アドレスで示された送信元アドレス「E F G H」及びあて先アドレス「A B C D」に対応する共通アドレスを取得する。制御部 3 4 3 は、送信側 A T M アドレスで示された送信元アドレス「E F G H」を、取得した共通アドレス「5 6 7 8」に、送信側 A T M アドレスで示されたあて先アドレス「A B C D」を、取得した共通アド

レス「1234」に、一度変換する。次に、制御部343は、テーブル344aを参照して、共通アドレスで示された送信元アドレス「5678」及びあて先アドレス「1234」に対応する提供側ATMアドレスを取得する。制御部343は、共通アドレスで示された送信元アドレス「5678」を、取得した提供側ATMアドレス「efgh」に、共通アドレスで示されたあて先アドレス「1234」を、取得した提供側ATMアドレス「abcd」に変換する。最後に、制御部343は、送信元アドレスやあて先アドレスを変換した要求データや指示データを含むパケットをI/F342に入力し、パケットを提供側ATM網320を介して情報提供部10に転送する。

#### 【0106】

同様に、制御部343は、I/F342から、提供側ATM網320を介してルータ340が受信した映像データを含むパケットを入力されると、テーブル344aを参照して、映像データに付加されている送信元アドレスが、テーブル344aが保持する提供側ATMアドレスで示された情報提供部10のアドレスの中にあるか否かを判断する。図10の場合、制御部343は、送信元アドレスがテーブル344aに保持された情報提供部10のアドレス「abcd」と一致する場合、映像データが情報提供部10から送信されたデータであると判断する。

#### 【0107】

次に、制御部343は、テーブル344aを参照して、提供側ATMアドレスで示された送信元アドレス「abcd」及びあて先アドレス「efgh」に対応する共通アドレスを取得する。制御部343は、提供側ATMアドレスで示された送信元アドレス「abcd」を、取得した共通アドレス「1234」に、提供側ATMアドレスで示されたあて先アドレス「efgh」を、取得した共通アドレス「5678」に、一度変換する。

#### 【0108】

次に、制御部343は、テーブル344bを参照して、共通アドレスで示された送信元アドレス「1234」及びあて先アドレス「5678」に対応する送信側ATMアドレスを取得する。制御部343は、共通アドレスで示された送信元アドレス「1234」を、取得した送信側ATMアドレス「ABCD」に、共通

アドレスで示されたあて先アドレス「5 6 7 8」を、取得した送信側 A T M アドレス「E F G H」に変換する。最後に、制御部 3 4 3 は、送信元アドレスやあて先アドレスを変換した映像データを含むパケットを I / F 3 4 1 に入力し、パケットを送信側 A T M 網 3 5 0 を介してストリーミングサーバ 6 0 に転送する。

#### 【0109】

尚、制御部 3 4 3 は、送信側 A T M 網 3 5 0 を介してルータ 3 4 0 が受信したデータに付加されている送信元アドレスが、テーブル 3 4 4 b が保持するストリーミングサーバ 6 0 の送信側 A T M アドレスと一致しない場合、そのデータを転送せずに破棄する。同様に、制御部 3 4 3 は、提供側 A T M 網 3 2 0 を介してルータ 3 4 0 が受信したデータに付加されている送信元アドレスが、テーブル 3 4 4 a が保持する情報提供部 1 0 の提供側 A T M アドレスの中に含まれていない場合、そのデータを転送せずに破棄する。

#### 【0110】

更に、制御部 3 4 3 は、図 2 に示した制御部 4 3 と同様に、情報提供部 1 0 からの映像データを同時に転送するデータ量の閾値を保持している。そして、制御部 3 4 3 は、図 2 に示した制御部 4 3 と同様にして、提供側 A T M 網 3 2 0 を介してルータ 3 4 0 が受信した映像データのデータ量と閾値とを比較し、その比較結果に基づいてデータの転送を制御する。この点については、図 2 に示した制御部 4 3 と実質的に同様であるため、ここでは説明を省略する。

#### 【0111】

このような本実施形態に係る通信システム 3 0 1 や通信システム 3 0 1 を用いた通信方法によれば、図 1 に示す通信システム 1 や通信システム 1 を用いた通信方法による効果とほぼ同様の効果を得ることができる。特に、ルータ 3 4 0 は、ストリーミングサーバ 6 0 から情報提供部 1 0 に送信された要求データや指示データに付加されている送信側 A T M アドレスを、共通アドレスに変換し、その変換した共通アドレスを提供側 A T M アドレスに変換する。又、情報提供部 1 0 からストリーミングサーバ 6 0 に送信された映像データに付加されている提供側 A T M アドレスを共通アドレスに変換し、その変換した共通アドレスを送信側 A T M アドレスに変換する。そのため、情報提供部 1 0 及び提供側 A T M 網 2 2 0 と

、ストリーミングサーバ60及び送信側ATM網350は、それぞれ独自のアドレス体系を保ったまま、ルータ340を介して接続することができる。その結果、アドレス体系の統一を行う必要がなく、より低コストで通信システム301を構築することができる。

#### 【0112】

##### 〔変更例〕

本発明は、上記実施形態に限定されるものではなく、種々の変更が可能である。上記実施形態では、情報提供手段である映像提供部10、映像提供部(A)10a、映像提供部(B)10bは、情報データとして映像データを提供しているが、情報提供手段が提供する情報データは、映像データに限られない。例えば、情報提供手段は、情報データとして、音声データやテキストデータ、静止画データ等を提供することができる。

#### 【0113】

又、制御部43は、提供側VPN20を介してルータ40が受信した映像データのデータ量と閾値との比較結果に基づいてデータの転送を制御する際に、ストリーミングサーバ60からの要求データは情報提供部10に転送してしまい、情報提供部10からの映像データの転送を制限するようにしてもよい。具体的には、制御部43は、提供側VPN20を介してルータ40が受信した映像データのデータ量が閾値未満の場合には、情報提供部10からの映像データをストリーミングサーバ60に転送する。一方、制御部43は、提供側VPN20を介してルータ40が受信した映像データのデータ量が閾値以上となった場合には、現在、映像データの提供を行っていない新たな情報提供部10に対するストリーミングサーバ60からの要求データに対して、映像提供部10が送信した映像データの転送を行わない。更に、制御部43は、映像提供部10に対して、映像データの転送を拒否する通知を行う。

#### 【0114】

この場合、ストリーミングサーバ60は、一定時間経過しても要求データや指示データに対する映像データを受信できないため、再度、要求データや指示データの送信を行う。そして、再度送信した要求データや指示データに対する映像デ

ータの送信が、更に一定時間経過してもない場合には、ストリーミングサーバ60は、現在、ネットワークが混雑していて映像データの提供ができないと判断する。そして、ストリーミングサーバ60は、携帯端末70に対して、現在、混雑していて映像データの提供ができないことを通知する。

#### 【0115】

又、図1、図7、図9に示す通信システム1, 201, 301において、送信側VPN50及びストリーミングサーバ60, 260や、送信側ATM網350及びストリーミングサーバ60を複数設けてもよく、その場合に、ルータ40, 240, 340を、複数の送信側VPN50や送信側ATM網350毎に設けてもよい。又、図1、図7、図9に示す通信システム1, 201, 301のようにストリーミングサーバ6, 260が1つの場合に、複数のルータ40, 240, 340を設けるようにしてもよい。又、図7に示す通信システム201において、ルータ240を、複数の提供側VPN(A)20a、提供側VPN(B)20b毎に設けてもよい。又、図9に示す通信システム301も、図7に示す通信システム201のように、提供側ネットワークである提供側ATM網320を複数備えるようにしてもよい。

#### 【0116】

更に、図7に示す通信システム201において、提供側VPN(A)20aと提供側VPN(B)30bとを1つのネットワークに接続し、提供側VPN(A)20aと提供側VPN(B)30bは、そのネットワークを介してルータ240と接続するようにしてもよい。例えば、集合住宅や複数のテナントが入居しているビル等において既存のネットワークが存在する場合、複数の提供側ネットワークを既存のネットワークに接続し、複数の提供側ネットワークは、そのネットワークを介してルータと接続するようにしてもよい。これによれば、例えば、各提供側ネットワークが接続するネットワークの伝送速度が、各提供側ネットワークの伝送速度よりも速い場合には、情報提供部は、提供側ネットワークを介して送信する場合に比べて、効率よく映像データ等の容量の大きい情報データを送信することができる。尚、図9において、提供側ATM網320内、送信側ATM網350内の両方、又は、提供側ATM網320内、送信側ATM網350内の

いずれか一方に、ルータ 340 の機能を備える ATM 交換機を設けるようにしてもよい。

#### 【0117】

#### 【発明の効果】

以上説明したように、本発明によれば、情報データを提供する情報提供側と、その情報提供側から取得した情報データを端末に送信する情報送信側とが、独自のセキュリティポリシーを保つことができ、低コストで構築可能なセキュリティの高い通信システム及びその通信システムを用いた通信方法、並びに、その通信システムで用いられる転送装置及びプログラムを提供することができる。

#### 【図面の簡単な説明】

##### 【図 1】

本発明の第 1 の実施の形態に係る通信システムの構成を示す図である。

##### 【図 2】

本発明の第 1 の実施の形態に係るルータの構成を示すブロック図である。

##### 【図 3】

本発明の第 1 の実施の形態に係るアドレスの変換を説明する説明図である。

##### 【図 4】

本発明の第 1 の実施の形態に係るストリーミングサーバの構成を示すブロック図である。

##### 【図 5】

本発明の第 1 の実施の形態に係る映像提供部の構成を示すブロック図である。

##### 【図 6】

本発明の第 1 の実施の形態に係る通信方法の手順を示すフロー図である。

##### 【図 7】

本発明の第 2 の実施の形態に係る通信システムの構成を示す図である。

##### 【図 8】

本発明の第 2 の実施の形態に係るルータの構成を示すブロック図である。

##### 【図 9】

本発明の第 3 の実施の形態に係る通信システムの構成を示す図である。

## 【図10】

本発明の第3の実施の形態に係るルータの構成を示すブロック図である。

## 【図11】

従来の通信システムの構成を示す図である。

## 【符号の説明】

- 1, 201, 301, 401 通信システム
- 10 映像提供部
  - 10a 映像提供部 (A)
  - 10b 映像提供部 (B)
- 11, 410 カメラ
  - 11a カメラ (A)
  - 11b カメラ (B)
- 12 映像提供サーバ
  - 12a 映像提供サーバ (A)
  - 12b 映像提供サーバ (B)
- 20 提供側VPN
  - 20a 提供側VPN (A)
  - 20b 提供側VPN (B)
- 21, 51, 321, 521 認証サーバ
  - 21a 認証サーバ (A)
  - 21b 認証サーバ (B)
- 30 提供側サーバ
  - 30a 提供側サーバ (A)
  - 30b 提供側サーバ (B)
- 40, 240, 340 ルータ
  - 41, 42, 61, 62, 121, 122, 241, 242a, 242b, 341, 342 I/F
  - 43, 243, 343 制御部
  - 44, 244a, 244b, 344a, 344b テーブル

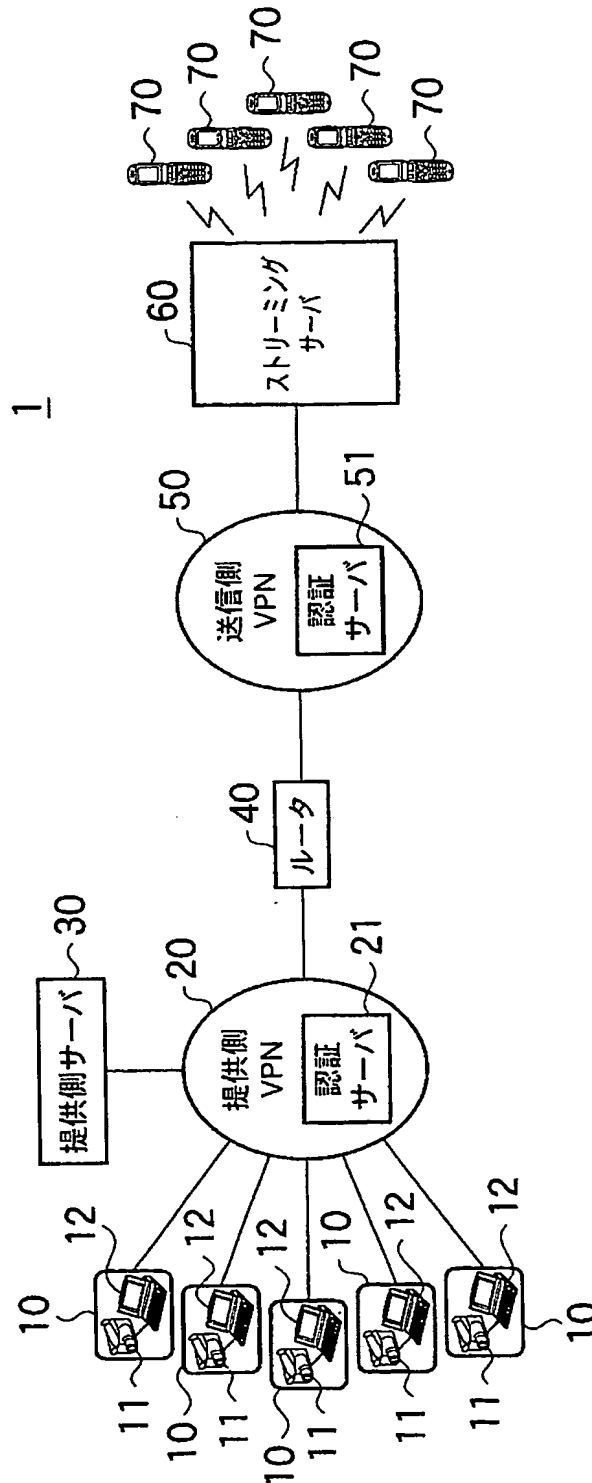


50 送信側VPN  
60, 260, 430 ストリーミングサーバ  
63 制御部  
64 データベース  
65 送信部  
70, 440 携帯端末  
70a 携帯端末(A)  
70b 携帯端末(B)  
101, 102, 103, 104 パケット  
123 制御部  
124 エンコーダ  
320 提供側ATM網  
350 送信側ATM網  
244, 344 データベース  
420 VPN

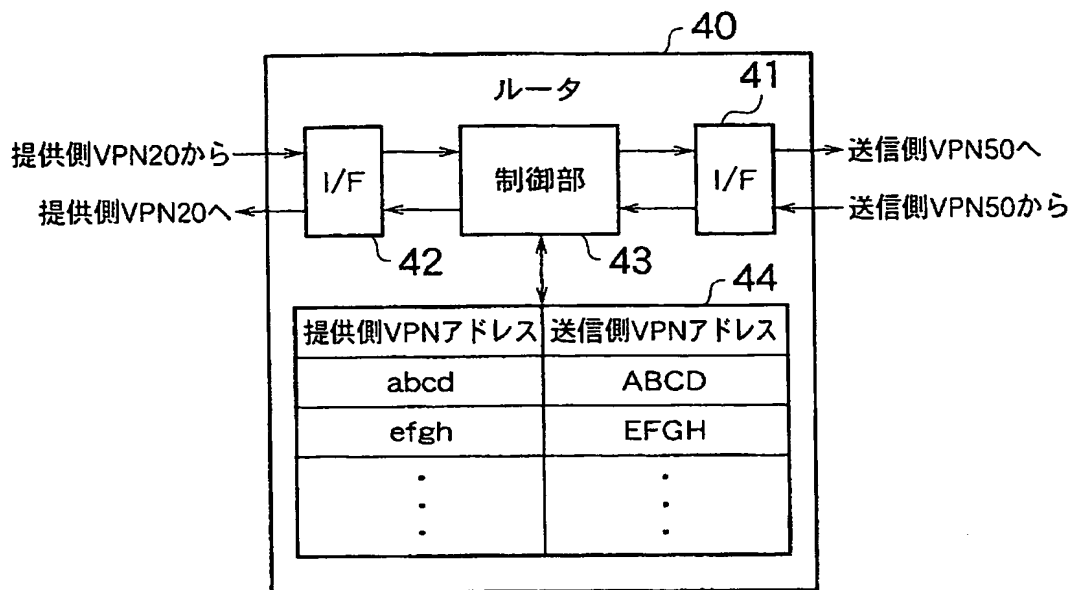
【書類名】

図面

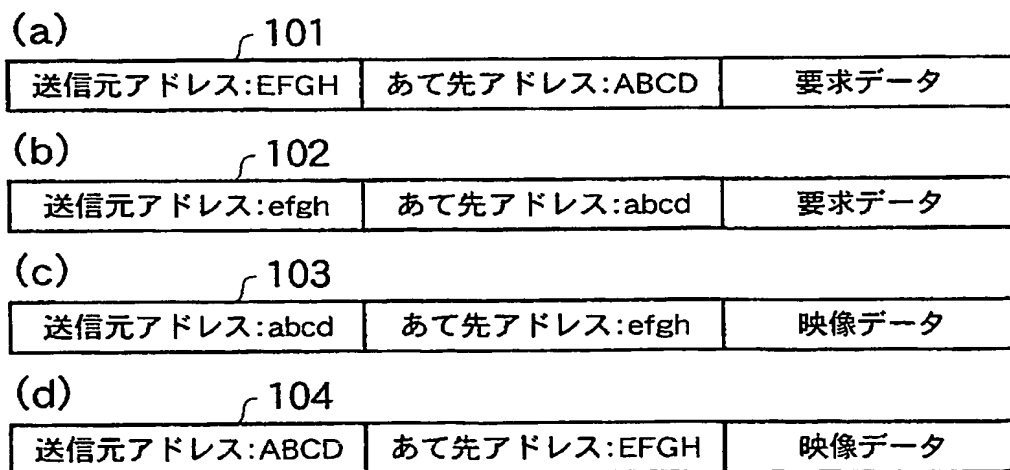
【図 1】



【図 2】

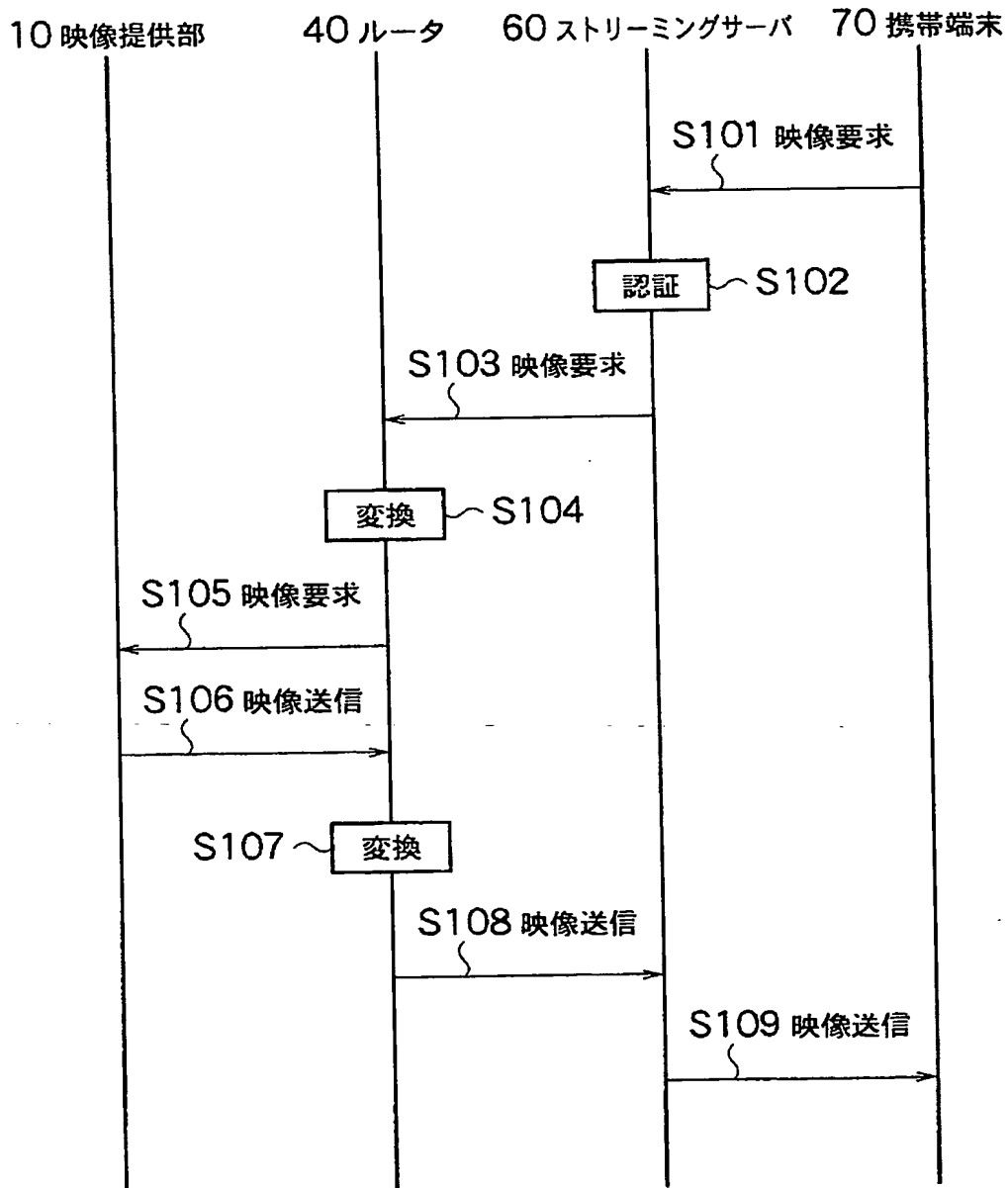


【図 3】

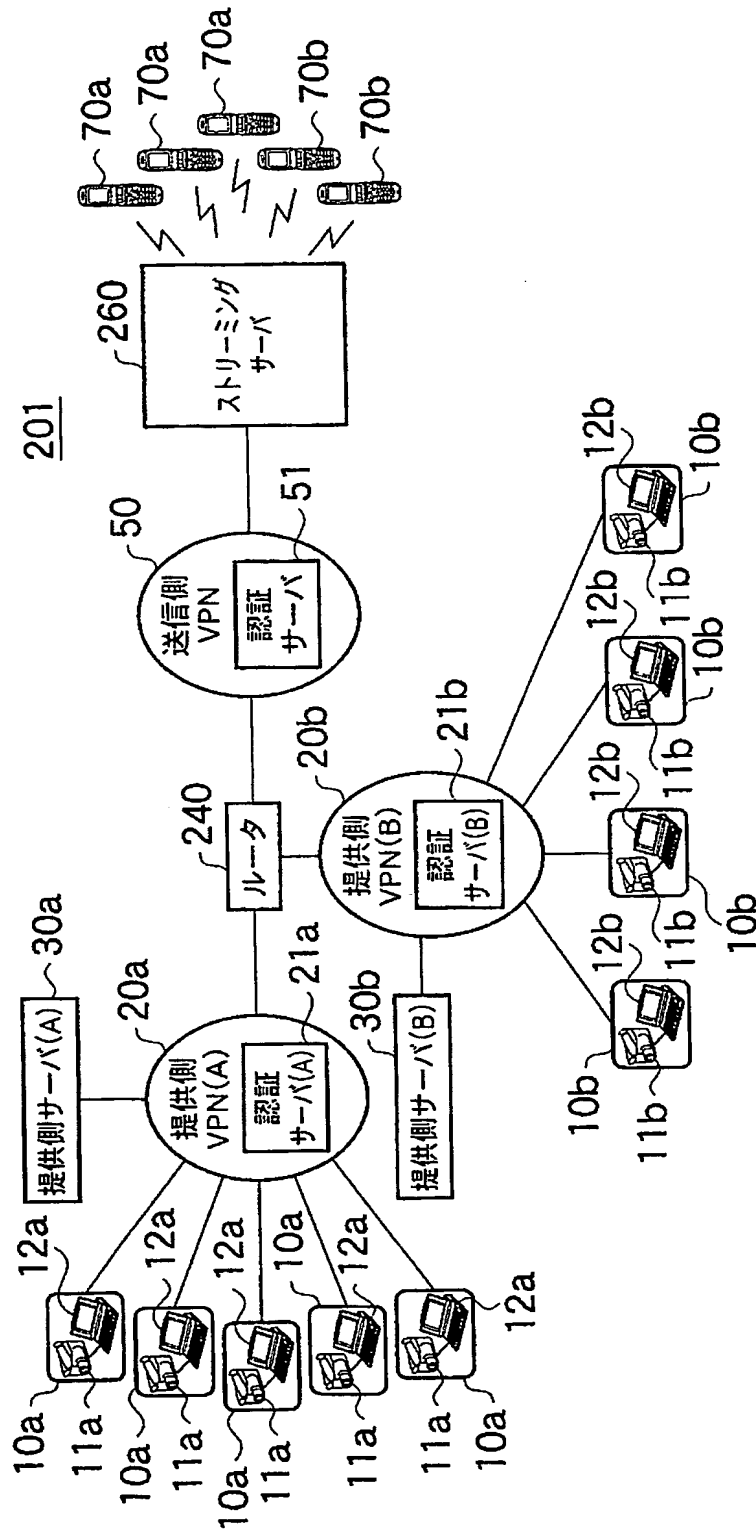




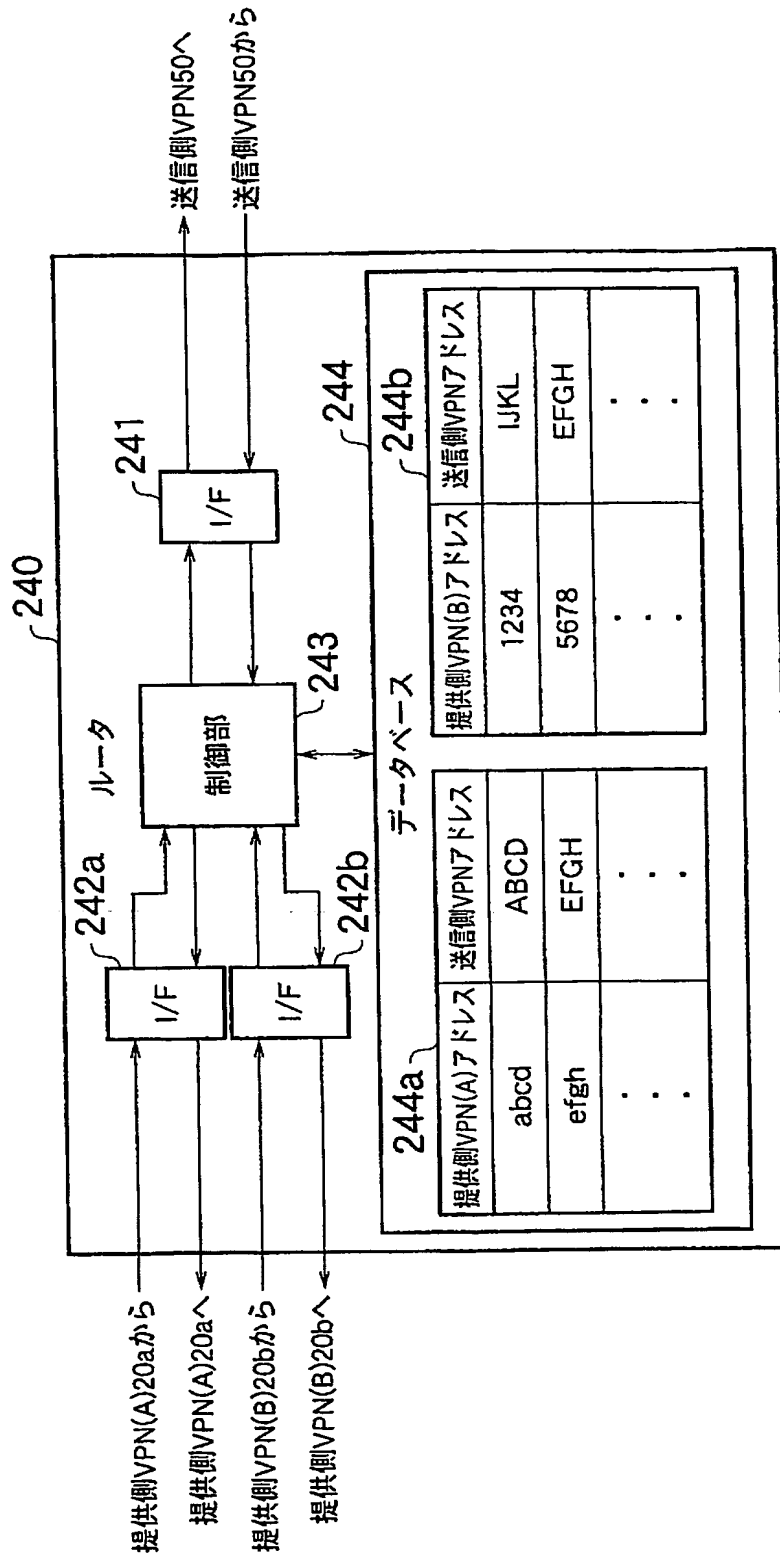
【図6】



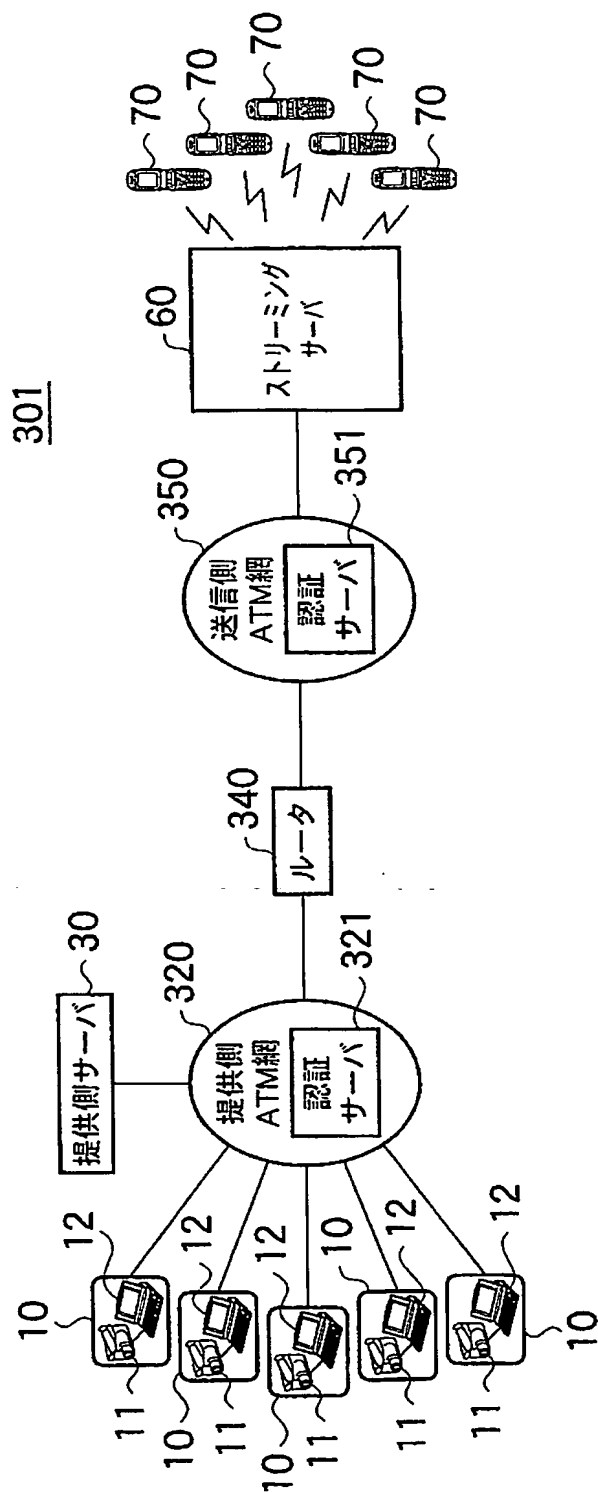
【図 7】



【図 8】

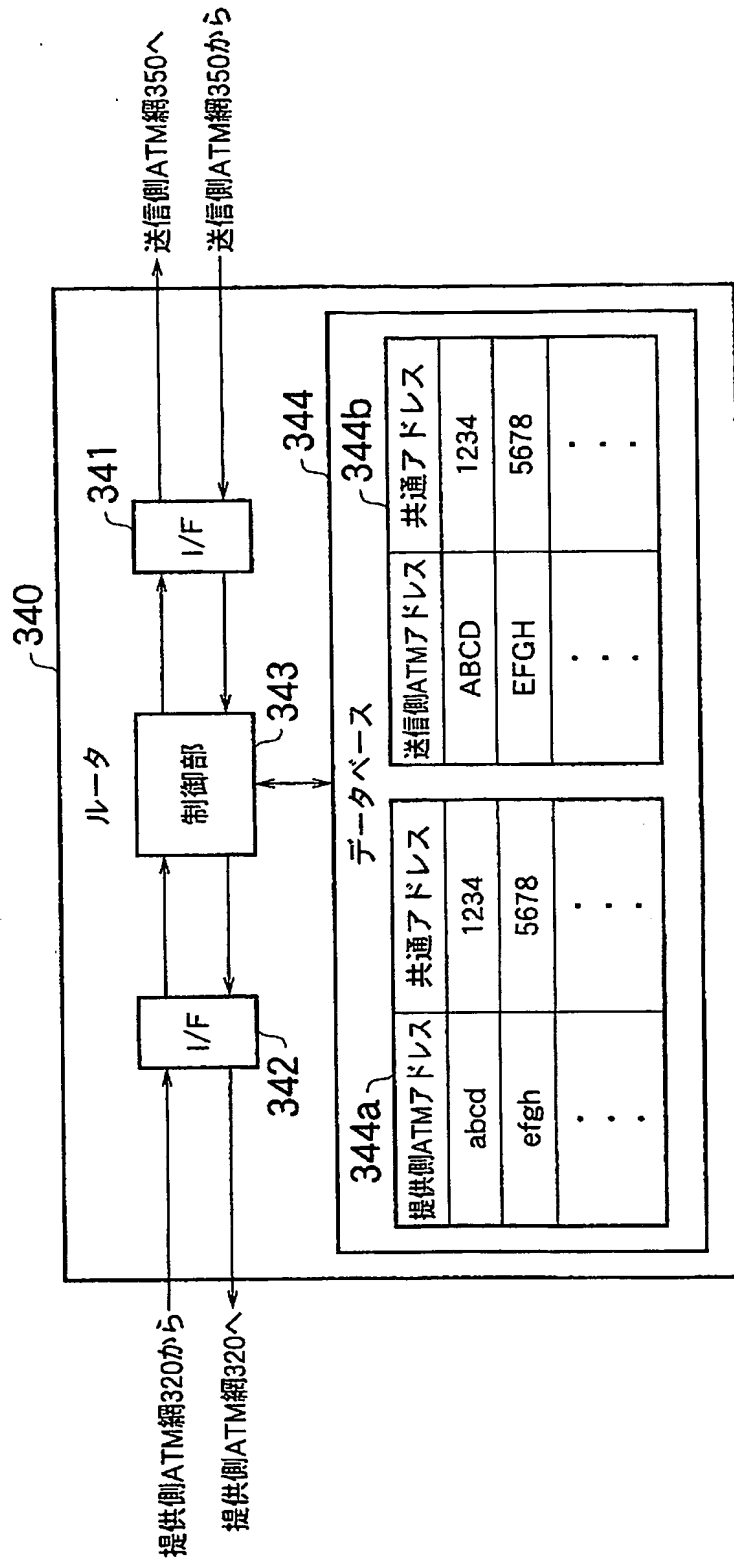


【図9】

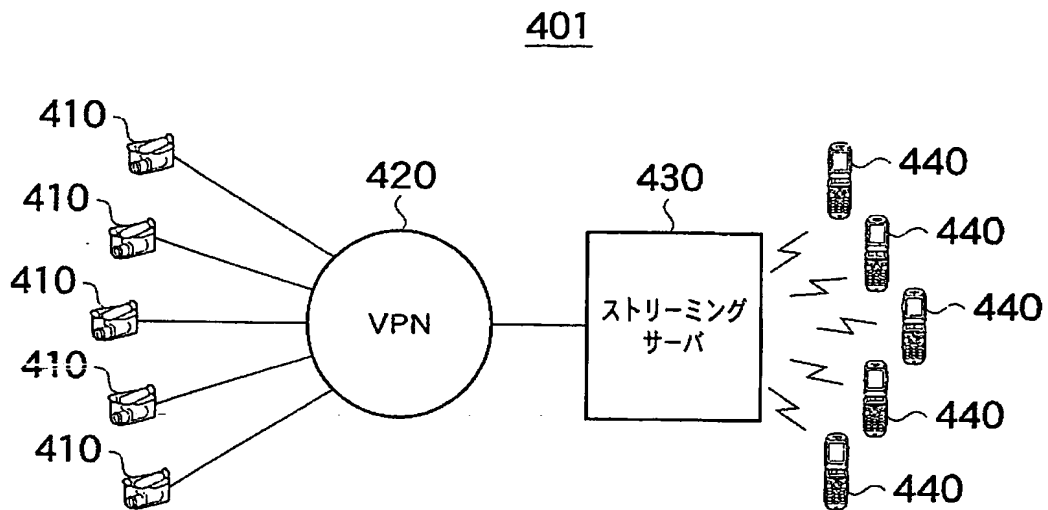




【図10】



【図 11】



【書類名】 要約書

【要約】

【課題】 情報データを提供する情報提供側と、その情報提供側から取得した情報データを端末に送信する情報送信側とが、独自のセキュリティポリシーを保つことができ、低コストで構築可能なセキュリティの高い通信システムを提供する。

【解決手段】 映像提供部 10 はアクセス制限がされた提供側 VPN 20 に接続し、ストリーミングサーバ 60 は、アクセス制限がされた送信側 VPN 50 に接続する。ルータ 40 は、送信側 VPN 50 を介して受信した要求データや指示データがストリーミングサーバ 60 から送信されたデータであるか否かを判断し、提供側 VPN を介して受信した映像データが情報提供部 10 から送信されたデータであるか否かを判断し、それらの判断結果に基づいて、送信側 VPN 50 を介して受信したデータや提供側 VPN 20 を介して受信したデータの転送を行う。

【選択図】 図 1

特願 2002-303494

出 願 人 履 歴 情 報

識別番号

[392026693]

1. 変更年月日  
[変更理由]

2000年 5月19日

名称変更

住所変更

住 所  
氏 名

東京都千代田区永田町二丁目11番1号  
株式会社エヌ・ティ・ティ・ドコモ